Transportation Security Administration

Transportation Security Administration
Office of Law Enforcement/Federal Air Marshal Service
Security Services and Assessments

SSI Policies & Procedures Handbook

Attachment to TSA MD 2810.1

Version 2.0

SSI Program
Current as of November 4, 2015

Document Change History

Version	Date	Description
1	23 April 2012	Draft Baseline Release - ***Note:*** *This revised policy superseded all SSI Program office policies and procedures dated September 29, 2006 and August 7, 2007.*
2.0	4 November 2015	This revised policy supersedes Version 1 of the SSI Policies & Procedures Handbook. Updated links to SSI Program resources; expanded guidance on *SSI Challenge and Appeals Process* (Subsection 3.8); inclusion of guidance on transmitting images in Good software (Subsection 5.2.3); added guidance on *Video Teleconferencing* (Subsection 5.2.8); updated guidance on encrypting files using Adobe® Acrobat® Professional, Microsoft® Office®, and WinZip® (Subsection 5.3.3); included provision for sharing/disclosing SSI with those receiving classified information (Subsection 6.1); added guidance *Disclosure of SSI to AFGE and Personal Representatives* (Subsections 6.1 and 6.3); included expanded guidance on delegation of authority for disclosure of SSI to Congress (Subsection 6.4); added guidance *State Open Records Requests* (Subsection 6.6); removed reference to *SSI Site Assistance Visits* (Subsection 9.7); added decision process for *Determining SSI Release to Foreign Governments* (Appendix 8); added instructions for new and certified SSI Coordinators (Appendix 9 & 10); added instructions for applying Watermarking to files (Appendix 11); added instructions for Formal Appeal Justification (Appendix 12).

EFFECTIVE DATE AND IMPLEMENTATION: These changes are effective immediately upon signature.

Annmarie Lontz
Division Director
Security Services and Assessments Division
Office of Law Enforcement/Federal Air Marshal Service

November 4, 2015
Date

Table of Contents

Appendices

1.0 Introduction

Welcome to the Sensitive Security Information (SSI) Policies and Procedures (P&P) Handbook. This Handbook expands on the SSI Regulation (49 C.F.R. Part 1520, *Protection of SSI*); DHS MD 11056.1, *Sensitive Security Information*; DHS MD 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*; and TSA MD 2810.1, *SSI Program*.

What is SSI?

SSI is a category of sensitive but unclassified (SBU) information that must be protected because it is information that, if publicly released, would be detrimental to the security of transportation.[1] In other words, SSI is information that could be used to bypass or defeat transportation security measures. Armed with SSI, our adversaries will be empowered. (For detailed categories of SSI, *see* the SSI Regulation, 49 C.F.R. § 1520.5(b)(1) through (16)).[2] For additional guidance on how to identify SSI, see the SSI Program office Identification Guides.

Purpose

This Handbook contains policies and procedures on how to properly identify, mark, handle, protect, disclose, and destroy SSI. This Handbook covers many media that may contain SSI, including hard copy (paper), soft copy (electronic), magnetic, CDs and DVDs, video, and other types of media (written and spoken). If a topic of interest is not covered in this Handbook, contact the SSI Program office at SSI@tsa.dhs.gov for consideration of inclusion in future SSI P&P Handbook updates or in the SSI Program office Frequently Asked Questions (FAQ).

During periods of national emergency or exigent circumstances, the TSA Administrator or SSI Program Chief may determine that certain requirements of this Handbook should be temporarily suspended.[3] Even during national emergency or exigent circumstances, however, all covered persons are still required to take reasonable measures to protect SSI.

Who Should Use this Handbook?

All persons permanently or temporarily assigned, attached, detailed to, employed by, or under contract with TSA (including interns and foreign nationals) must follow the guidance in this Handbook and are hereafter referred to generally as "personnel," unless otherwise specified. While this Handbook was specifically designed for TSA personnel, it may also serve as a model for use by other DHS components.

This Handbook may also be used as a collection of best practices for non-DHS persons who handle SSI. These persons include air carriers; airport operators; other Federal agencies; state, local, and tribal governments; and other covered persons as defined in 49 C.F.R. § 1520.7. For consideration of sharing this Handbook outside of the Department of Homeland Security (DHS), contact the SSI Program office directly at SSI@tsa.dhs.gov for a determination on a case-by-case basis.

---

[1] Under 49 C.F.R. § 1520.5(a), the SSI Regulation also provides other reasons for protecting information as SSI beyond that the release of the information would be detrimental to the security of transportation. TSA, however, primarily uses the criterion of "detrimental to the security of transportation" when determining whether information is SSI.

[2] All future "§" references refer to sections in the SSI Regulation, 49 C.F.R. Part 1520.

[3] Even if SSI Program office policies or procedures are temporarily suspended, other TSA program offices (e.g., Office of Information Technology's Information Assurance Division (IAD)) may have policies that still need to be followed.

2.0 Definitions (In alphabetical order)

Authorized Redactor
A TSA employee who has been authorized in writing by an Assistant Administrator or equivalent to redact documents and/or perform quality assurance reviews on documents redacted by another Authorized Redactor at TSA.

Coordinators

SSI Coordinator
A TSA employee who has been appointed by the Deputy Administrator, an Assistant Administrator or equivalent, a Federal Security Director, or a Supervisory Air Marshal in Charge to be a primary or alternate point of contact for the SSI Program office.

Certified SSI Coordinator
An SSI Coordinator who has (1) completed the required modules of Advanced SSI Training, (2) passed the SSI Certification Exam, and (3) properly maintained their certification status by completing Continuing Education in SSI (CESSI) Training on an annual basis.

SSI Area Coordinator
A Certified SSI Coordinator who is appointed by the SSI Program Chief (with approval from the Coordinator's Federal Security Director (FSD) or Supervisory Air Marshal in Charge (SAC) where the Area Coordinator is based). An Area Coordinator serves as the point of contact (POC) for SSI Coordinators in the field in geographic regions defined by the SSI Program Chief.

Covered Persons
As defined in the SSI Regulation, at § 1520.7, an individual or entity that has transportation security or transportation security-related responsibilities to include, but not limited to, (1) anyone who is permanently or temporarily assigned, attached, detailed to, employed by, or under contract with DHS, (2) regulated parties, Federal, State, Local and tribal government employees, contractors, and grantees, as well as TSA stakeholders and industry partners; (3) Committees of Congress; (4) other persons with a need to know as defined in § 1520.11; and (5) persons receiving SSI pursuant to other conditional disclosures. *See also* "Need to Know."

Destroy
The process of making a record, whether paper materials, electronic medium (drive, CD, etc.), or other record medium, containing SSI unreadable, unrecognizable, and unusable.

Disclose
The act of providing access to a record containing SSI to a covered person with a need to know or others who are authorized in writing by the TSA Administrator or designee to have access to SSI.

Identifying SSI

Determination
A decision made by the DHS Secretary, TSA Administrator (also known as the Assistant Secretary for TSA) or designee whether to identify information as SSI which has not previously been evaluated for SSI.

Identification Guides
SSI Program office-issued guidance, created in coordination with subject matter experts (SMEs), to help authorized redactors or other personnel identify SSI pursuant to § 1520.5(b).

Loss of SSI Designation
Information loses its SSI designation when the TSA Administrator, or designee, determines in writing pursuant to § 1520.5(c) that the information once protected as SSI under § 1520.5(b) no longer is detrimental to transportation security.

Redaction (R)
To obscure or prevent portions of a record containing SSI from being viewed and accessed. Adobe® Acrobat® Professional is TSA's standard software tool for electronic document redaction. Redaction of hard copy documents must follow the manual redaction procedures described in Section 7(C) of TSA MD 1400.17, *Document Redaction.*

SSI Advanced Application Guide
Guidance developed by the SSI Program office designed to assist in conducting an SSI Assessment to determine whether a record contains SSI.

SSI Assessment
An evaluation of whether a record contains SSI.

SSI Review
An evaluation of a record by the SSI Program office to identify and mark SSI within the record and cite the specific subsection(s) of 49 C.F.R. § 1520.5(b) that justifies the determination.

SSI Reviewers' Guide
Guidance developed by the SSI Program office designed to assist in conducting SSI Reviews. The SSI Reviewers' Guide provides more detail and analytical precedent than the SSI Advanced Application Guide.

Visual Redaction (VR)
The process of visually identifying SSI in a record. This process does not actually remove or obscure the data within the record, as with a redaction, but it allows for the accurate application of redactions to a document in the future.

Incidents

Password Incident

When either (1) a password created to encrypt SSI is inappropriately shared with covered persons in a manner not in accordance with this TSA SSI P&P Handbook; or (2) the Standard TSA Password is shared inappropriately with persons not within DHS.

SSI Incident

The verified or suspected loss, breach, or unauthorized disclosure of SSI to non-covered persons; the unauthorized disclosure of SSI to covered persons who do not have a need to know the information; or the non-compliance with the TSA SSI Policies & Procedures Handbook in the handling of a record containing SSI.

Marking

Applying the SSI protective marking (SSI header) and distribution limitation statement (SSI footer) to materials containing SSI in accordance with the SSI Regulation, at § 1520.13. Some circumstances may require variations in marking as further detailed in Section 4.0 *Marking SSI* of this Handbook.

Need to Know

Generally, a person or entity has a need to know SSI when access to the SSI is necessary to carry out transportation security activities or to perform official duties as defined in the SSI Regulation at § 1520.11. For specific SSI, the TSA Administrator or designee may make a finding that only specific persons or classes of persons have a need to know.

Protect

Taking required and other reasonable steps, as defined in the SSI Regulation at § 1520.9 and this TSA SSI P&P Handbook, to safeguard a record containing SSI and prevent disclosure to non-covered persons or persons without a need to know.

Record

Any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term record, for the purposes of SSI protection, also includes any draft, proposed, or recommended change to any record.

Sensitive Security Information

As defined in the SSI Regulation at § 1520.5, information obtained or developed in the conduct of security activities, including research and development, the disclosure of which DHS/TSA has determined would, among other things, be detrimental to the security of transportation.

Share

See "Disclose."

SSI Impact Assessment (SSIIA)

A document prepared by a program office or system owner in conjunction with the SSI Program office and the Office of Information Technology's Information Assurance and Cyber Security Division to assess the security in place to protect SSI and resultant risk associated for an IT system. This document may also be used by other non-TSA systems or other secure sites not requiring Security Authorization to document alternate acceptable protection in lieu of standard SSI policies and procedures.

SSI System

Any system that processes, stores, or transmits SSI information. A system's SSI status shall be reflected in its SSI Threshold Analysis (SSITA) document.

SSI Training

Basic SSI Training/SSI Awareness Training

Training on SSI to educate covered persons about the principles of identifying, marking, safeguarding, disclosing, and destroying SSI, developed or endorsed by the SSI Program office.

Advanced SSI Training

TSA training on SSI, which is developed and provided by the SSI Program office. Completion of all specified advanced SSI training modules is required before an appointed SSI Coordinator or other covered person may take the SSI Certification Examination.

SSI Certification Examination

An examination provided to covered persons who have completed all required modules of Advanced SSI Training. Covered persons who pass the examination achieve the status of "SSI Certified."

CESSI

Continuing Education in SSI training. Certified SSI Coordinators and others who have passed the SSI Certification Exam must complete CESSI requirements annually to maintain SSI Certification.

SSI Certified

Any covered person who has (1) completed the required modules of Advanced SSI Training, (2) passed the SSI Certification Exam, and (3) properly maintained their certification status by completing CESSI training on an annual basis. *See also* "Certified SSI Coordinator."

SSI Threshold Analysis (SSITA)

A document prepared by a program office or system owner in conjunction with the SSI Program office and the Office of Information Technology's Information Assurance and Cyber Security Division to determine if an IT system processes, transmits or stores SSI. This document is produced as part of the Security Authorization process. This document shall also be used for emerging and standing security programs and initiatives to determine whether it may be appropriate to develop an SSI Identification Guide for the program in coordination with the SSI Program office.

Standard TSA Password

A password generated by the SSI Program office which may be used by TSA personnel to encrypt SSI. This password may be obtained through the designated SSI Coordinator.

Subject-Matter Expert (SME)

A person who has expert-level knowledge and information about specific transportation security matters who can assist in determining the specific program-related information that is SSI.

TSA Personnel

Persons permanently or temporarily assigned, attached, detailed to, employed by, or under contract with TSA (including interns and foreign nationals).

3.0 Identifying SSI

3.1 Creating SSI Identification Guidance

The information defined as SSI within the SSI Regulation is general in nature and often subject to interpretation. As the arbiter of what is SSI, the SSI Program office issues SSI Identification (ID) Guides on precisely what information is and is not SSI within a specific subject area and defining which subsections of the SSI Regulation apply. All SSI ID Guides are developed in collaboration with SMEs and are updated periodically as information and programs change. ***Note:*** *In order to have accurate SSI ID Guides, full participation and prompt communication from the relevant program office SSI Coordinator(s) and designated SMEs are necessary.*

An SSI ID Guide is generally created after repeated requests to review or make SSI determinations on a particular subject matter. Certain new programs or agency efforts have SSI implications, necessitating the development of an SSI ID Guide at the outset of the program. Furthermore, the development or revision of a TSA Security Classification Guide (SCG) often prompts the creation of, or amendments to, a corresponding SSI ID Guide. ***Note:*** *The SSI Threshold Analysis template (see subsection 11.0 Determining SSI Systems and Appendix 6, SSI Threshold Analysis) may also be used by standing and emerging security programs and initiatives to determine whether it may be appropriate to develop an SSI ID Guide in coordination with the SSI Program office.*

After a subject area is identified as appropriate for an SSI ID Guide, the SSI Program office works through the SSI Coordinator network to identify appropriate SMEs for the subject area. SMEs help identify what information about the program or subject matter should be protected as SSI.

The SSI Program office then conducts research into the identified topics to determine what information does not warrant protection. Of the remaining information, the SSI Program office determines if the information falls within the scope of one or more of the 16 categories of the SSI Regulation. Information not covered in § 1520.5(b)(1) through (15), or in an existing (16) determination, is considered for a new (16) determination.

See Appendix 1: *SSI Program Initial Decision Flow Chart* for additional information about how the SSI Program office conducts initial determinations on what may be protected as SSI under the SSI Regulation.

3.2 Using SSI Identification Guidance

SSI ID Guides serve as a resource for personnel to recognize whether information requires protection as SSI. ID Guides are intended for wide distribution throughout DHS. The SSI ID Guides are designed for use both by persons with great familiarity with the SSI Regulation and SSI ID Guides, and by persons with little familiarity with either.

All personnel are responsible for using SSI Program office-issued SSI ID Guides to recognize if the material they are handling may contain SSI. ***Note:*** *To verify the content does not contain SSI before posting to the Internet or releasing to a non-covered person, see subsections 3.3 Conducting SSI Assessments and 5.2.1 The Internet.*

Personnel with questions about whether information is SSI should first determine whether a relevant SSI ID Guide exists and verify whether the information is or is not SSI. If the information appears not to be SSI, personnel shall consult with their SSI Coordinator for verification through an SSI Assessment. Personnel shall also refer to the SSI ID Guides to determine whether to mark and protect a record as SSI, when they are reviewing a record for SSI content, or when they have come into possession of a record that they believe is not properly marked. Within the SSI Program office, SSI ID Guides assist in conducting SSI Assessments and SSI Reviews, and serve as one authority for SSI determinations.

For consideration of sharing the SSI ID Guides beyond DHS, contact the SSI Program office directly at SSI@tsa.dhs.gov for a determination on a case-by-case basis.

3.3 Conducting SSI Assessments

An SSI Assessment is an evaluation of whether a record contains SSI. An official SSI Assessment of a record that may contain SSI can only be completed by SSI Certified personnel. SSI Assessments must be completed using the appropriate SSI ID Guide(s) (see subsection 3.2 *Using SSI Identification Guidance* for more information).

In no case should information be assessed as SSI to:

- Conceal a violation of law, inefficiency, or administrative error; or
- Prevent embarrassment to any person, organization, or agency.

If there is not enough information available in the SSI Regulation, the SSI Advanced Application Guide, the SSI Reviewers' Guide, and the SSI ID Guides to make a confident SSI Assessment, personnel shall contact the SSI Program office at SSI@tsa.dhs.gov for additional assistance and to provide recommendations for possible SSI ID Guide updates.

3.4 Conducting SSI Reviews

An SSI Review is an evaluation of a record to identify and mark the SSI within the record. Only TSA employees assigned to the SSI Program office may conduct final SSI Reviews. A final SSI Review conducted by the SSI Program office is required before redactions of SSI may be applied by an Authorized Redactor.

The SSI Program office conducts a three-level review process to protect against the over-protection or improper release of SSI. If redactions are applied to the record, an independent reviewer conducts a quality assurance check for the security of the electronic redactions after the final review is completed.

Certified SSI Coordinators are authorized to conduct the first-level SSI Review for CESSI credit (see subsection 8.0, *SSI Training Programs*, for more information on the CESSI Program) and must send their review findings to the SSI Program office for the second- and final-level reviews, as well as a quality assurance check.

Personnel conducting an SSI Review must abide by the following general principles:

- Protect SSI on the merits of the particular information being reviewed, regardless of the requester of the information or the purpose of release.

- Release as much information publicly as possible without compromising transportation security. The following factors must be considered:
  - **Operational Use to Adversaries:** Would the information help them bypass or defeat transportation security measures or identify specific targets to plan or execute attacks?
  - **Level of Detail:** More detailed information is generally more useful and more likely to be SSI.
  - **Public Availability:** Has the Government released the information publicly in an official statement or document?
    Note: *Some partially-compromised (publicly or unofficially released) open source information may remain SSI because of its operational use to adversaries.*
  - **Obviousness:** Obvious or intuitive information is generally not protected as SSI unless its operational use to adversaries dictates otherwise.
  - **Age of the Record:** This factor may be overridden by the SSI reviewer's assessment of the current security implications (e.g., superseded, inactive screening procedures may still be SSI if they match or reflect current procedures) or potential future use of historical procedures.
- Redact the smallest possible portion of the record (word, phrase, or sentence) necessary to protect SSI, unless the entire document, page, or paragraph is SSI. Do not simply redact entire documents, pages, or paragraphs unless it is necessary (1) to prevent an inference of the redacted information, or (2) to prevent a cumulative SSI effect where the non-redacted portions of a document, when read in total, legitimately constitute SSI.
- Strive for consistency in SSI redactions (e.g., if information was redacted or released in a record previously reviewed for SSI, that information should be similarly or identically redacted or released in a record being currently reviewed, *unless* changes in SSI identification guidance, security measures, technology, or other factors make it necessary to redact the record differently).
- Protect SSI even when it is contained within a record not properly marked as SSI.
- Release in full (RIF) a record marked as SSI if it contains no SSI, unless other information protections (e.g., Privacy Act information) apply.

In no case should information be identified as SSI to:

- Conceal a violation of law, inefficiency, or administrative error; or
- Prevent embarrassment to any person, organization, or agency.

See Appendix 1: *SSI Program Initial Decision Flow Chart* for additional information on how the SSI Program office conducts initial determinations on what may be protected under the SSI Regulation. If there is not enough information available in the SSI Regulation, the SSI Advanced Application Guide, the SSI Reviewers' Guide, and the SSI ID Guides to conduct a confident SSI Review, Certified SSI Coordinators shall contact the SSI Program office at SSI@tsa.dhs.gov for additional assistance and to provide recommendations for possible SSI ID Guide updates.

3.5 Requesting an SSI Assessment or SSI Review from the SSI Program

Personnel shall use the following guidance to request that the SSI Program office conduct an SSI Assessment (when the program's SSI Coordinator cannot confidently conduct an SSI Assessment independently) or an SSI Review of material:

- Submit the SSI Review Request, available on the TSA SSI iShare page or from the SSI Program at SSI@tsa.dhs.gov.

  IMPORTANT: Do not include Classified National Security Information on the request (e.g., do not include titles containing Classified information)!

- Include in the request:
  - Your contact information;
  - The intended use of the document being submitted for review;
  - The document's page count;
  - How the material will be delivered to the SSI Program office, if other than as an attachment to the request;
  - Preference for a Visually Redacted (VR) or Redacted (R) end product, or both; and
  - The requested date of assessment or review completion.

3.6 Requesting an SSI Review of Classified Material from the SSI Program

Personnel shall use the following guidance to submit requests for the SSI Program office to review[4] classified material[5] for presence of SSI (*See also* subsection 3.5 *Requesting an SSI Assessment or SSI Review from the SSI Program*). This type of review typically occurs when the classified material is being considered for declassification, but may also occur to ensure appropriate marking within the classified document.

The requester must prepare the material to be reviewed as follows:

- Ensure the classified material is properly marked;
- Scan the material into a designated computer approved for handling classified material:
  - For Confidential and Secret material: Go to the Classified Processing Center (CPC)
  - For Top Secret material: Contact the SSI Program office for an alternate process;
- Save the file temporarily onto the designated computer desktop in PDF format;
- Encrypt each file on the desktop, using the current standard TSA password (see subsection 5.3.3 *Methods for Applying Encryption to SSI*);
- Burn the encrypted file onto a CD;
- Mark the CD with appropriate classification language, put the CD into a folder, and attach the appropriate classified Cover Sheet to the folder; and

[4] These instructions apply to requests for SSI reviews. SSI assessments of classified material may be made with hard copies which require attachment of a Cover Sheet for classified information (i.e., SF 704, SF 705, SF 703) during transport and placement into approved storage when left unattended.

[5] Requester acknowledges that an SSI review of classified material is not a declassification review and SSI may or may not overlap with classified information. If a declassification occurs after the SSI review, SSI may still remain in the document; therefore, the requester is encouraged to undertake a declassification review of the material *before* submitting it to the SSI Program office for SSI Review.

- Hand-deliver the folder containing the CD (or hard-copy) to the SSI Program office Analyst with whom delivery has been scheduled.

The SSI Program office logs the request to review the material once it receives a completed SSI Review Request. The SSI Program office Analyst(s) assigned to review the classified material either takes the folder to the CPC and prints out one copy of the material to use as the working copy or creates an SSI Program office copy of the CD and reviews the classified material on the designated classified computers in the CPC, making the appropriate redactions on the copy electronically. The Analyst saves program copies, (i.e. original, working, VR/R, etc.) onto the multi-session CDs that are stored in the safe as program documentation.

After review, the SSI Program office Analyst copies the VR/R onto the requester's properly marked and protected CD and arranges a time for pick-up with the requester.

3.7 Identifying Maritime SSI

For issues related to maritime SSI, contact the SSI Program office at SSI@tsa.dhs.gov. The SSI Program office consults with the United States Coast Guard (USCG) SSI Program Manager for resolution of the issue and notifies the requester of the result of discussions with the USCG SSI Program Manager. Requests for foreign disclosure of maritime-related SSI must be coordinated through the SSI Program office for ultimate approval by the USCG SSI Program Manager. For more information, see Appendix 8: *Determining SSI Release to Foreign Governments*.

3.8 SSI Challenge and Appeals Process

Any authorized recipient of SSI who believes the information has been improperly or erroneously marked as either SSI or not SSI (hereafter referred to as "challenger") is encouraged to challenge the marking. An appeal to the decision made by the recipient of the challenge may be filed with the TSA SSI Office. Challenges may be made either informally or formally.[6] Any decision to remove an SSI marking must be coordinated with the office which either applied the SSI marking or is programmatically responsible for the information (hereafter referred to as "information holder or owner") and the SSI Program office before the information may no longer be protected as SSI. All information under challenge or appeal will be protected as SSI until the process is complete.

3.8.1 SSI Challenge and Informal Appeals Process

Most questions regarding the appropriate marking for the information in question may be resolved through a challenge and/or informal appeal process.

- Informal challenges may be made directly by the challenger to the information holder or owner, who must then reevaluate the marking against the criteria in the SSI Regulation, at § 1520.5(b)(1) through (15) and implementing guidance published or approved by the SSI Program Chief available on iShare.[7]

[6] DHS MD 11056.1, Sensitive Security Information, III.F Challenging SSI.

[7] When uncertain whether information constitutes SSI, handle it as if it does and password-protect the attachment.

- The information holder or owner may request that the challenge be made formally, requiring the challenger to submit written justifications for change in marking using the process for formal appeals detailed in subsection 3.8.2, *Formal SSI Appeals Process*.
- When a formal or informal challenge does not result in a solution agreed upon by the challenger and information owner or holder, the challenger shall submit the material in question to the SSI Program office for a full SSI Review and determination.
- An informal appeal of SSI Program markings must be made directly to the SSI Program office (SSI@tsa.dhs.gov).
- Individuals submitting a challenge or appeal must not be subject to retribution for bringing such actions. Anonymity may be requested from any of the reviewers, and the reviewers must honor a challenger's request for anonymity and fully consider and appropriately process the challenge.

3.8.2 Formal SSI Appeals Process

Formal SSI Appeals to an SSI determination may be made to the SSI Program. The following process outlines the steps a challenger must take to initiate a formal appeal.

- Challengers shall submit formal SSI appeals in writing to the SSI Program office (SSI@tsa.dhs.gov).
- Formal appeal submissions should contain the word "Appeal" and the official review number in the subject line. Attached to the email, the challenger must include a table, see Appendix 12: *Formal Appeal Justification* for template, identifying the specific information at issue and the justification or rationale for the protection or release of that information. Rationales must be based upon the criteria in the SSI Regulation, at § 1520.5(b) implementing guidance published or approved by the SSI Program Chief available on iShare. The challenger may include documentation that speak to issues relevant to challenged information, i.e. reports indicating the sensitivity of the matter or level of public availability of the information.
- A senior SSI Program analyst will review the appeal documentation and solicit any necessary clarification or supporting documentation from the challenger within five (5) business days of initial receipt. The SSI Program will then provide the information holder or owner with a copy of the appeal documents.
- The information holder or owner must provide the SSI Program with a response denoting the justification or rationale for the protection or release of that information. Rationales must be based upon the criteria in the SSI Regulation, at § 1520.5(b)(1) through (15) or in the (16) determination, implementing guidance published or approved by the SSI Program Chief available on iShare. The challenger may include documentation that speaks to issues relevant to challenged information, i.e., reports indicating the sensitivity of the matter or level of public availability of the information. The response must be sent to the SSI Program within five (5) business days of receipt of the appeal documents.
- After receipt of the information holder or owner's response the SSI Program may solicit additional responses or comment from the parties. The SSI Program may provide preliminary opinions and attempt to obtain concurrence from all parties on protection determinations before issuing a final determination.

- The SSI Program Chief will evaluate the information gathered through the formal appeals process, including the rationale and justification provided, and will provide the final decision to both parties within five (5) business days after receipt of the information holder or owner's appeal response.
- Formal appeals originating outside of TSA should be submitted to the respective DHS component SSI Program Manager (hereafter referred to as "component manager"). Formal appeals of component managers' decisions, including intra-component challenges, are made to the TSA SSI Program as detailed herein.
- Formal appeal decisions of the SSI Program Chief may be appealed to the Administrator of the Transportation Security Administration.

3.8.3 Formal SSI Appeals Schedule

The SSI Program provides the following table as suggested schedule for handling appeals in order to address formal appeals in a timely manner. Challengers, information owners and the SSI Program shall strive to meet the following schedule when responding to SSI formal appeals.

FORMAL APPEALS PROCESS AND SCHEDULE	
Day	**Action**
Zero	**SSI Office Receives Appeal Document From Challenger**
1 - 5	*SSI Program may solicit additional information or clarifications from challenger.*
5	**Appeal Documents Provided To Information Holder Or Owner**
6-10	*SSI Program may solicit additional information or clarification from information holder or owner.*
10	**Holder or Owner Delivers Appeal Response to the SSI Program**
11-15	SSI Program will consolidate commentary, provide initial determination to both parties, attempt to obtain concurrence on initial determination, and/or solicit additional input from both parties.
15	**SSI Program Provides Formal Appeal Decision To Both Parties**

3.8.4 Final SSI Appeals

A further appeal of the decision made by the SSI Program Chief may be made to the Administrator of the Transportation Security Administration through the Executive Secretariat process. The decision of the Administrator is final and may not be appealed further. The SSI Chief will submit to the Administrator the documentation developed during the Formal Appeal and any additional documentation developed by the SSI Program or submitted by the Challenger.

4.0 Marking SSI

The creator of the record is primarily responsible for appropriately marking SSI. However, covered persons have a duty to mark SSI whether or not they created the records. Personnel who receive a record containing SSI that has not been properly marked must apply the SSI header and footer, and inform the creator and/or sender that the header and footer were missing. If unable to determine the creator/sender, personnel shall apply the header and footer and contact the SSI Program office at SSI@tsa.dhs.gov. Personnel disclosing SSI to covered persons who have a need to know must verify that the records containing SSI have the appropriate header and footer,[8] as shown below.

TSA encourages personnel handling SSI, both in paper and electronic form, to use the SSI Cover Sheet (DHS Form 11054), in addition to the header and footer required by the SSI Regulation as detailed below (*see also* subsection 4.1 *Marking Records & Media Containing SSI*).[9]

> **Header:** SENSITIVE SECURITY INFORMATION
>
> **Footer:** *WARNING:* This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. Parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. Parts 15 and 1520.

Personnel shall abide by the following when marking SSI contained in classified records:

- Do not comingle classified and Sensitive Security Information in the same paragraph;
- Apply SSI portion markings as (U/SSI) next to each paragraph/picture/area pertaining to SSI;
- Instead of the SSI header, add "SSI" to the end of the classification banner at the top and bottom of the page; and
- Apply the SSI footer to the bottom of the front page above the overall classification marking.

In no case should information be marked as SSI to:

- Conceal a violation of law, inefficiency, or administrative error; or
- Prevent embarrassment to any person, organization, or agency.

[8] The SSI header and footer are called the "protective marking" and the "distribution limitation statement," respectively, in the SSI Regulation at § 1520.13. For the purposes of this Handbook, the protective marking and the distribution limitation statement are referred to as the SSI header and footer.
[9] See also DHS MD 11056.1 for instruction on marking SSI for delivery to Congress.

4.1 Marking Records & Media Containing SSI

SSI markings shall be applied to different types of records and media as defined below. Personnel are also encouraged to use the SSI Cover Sheet (DHS Form 11054) on all documents and binders or folders containing SSI documents. See also Appendix 11: *Instructions for Watermarking Files*.

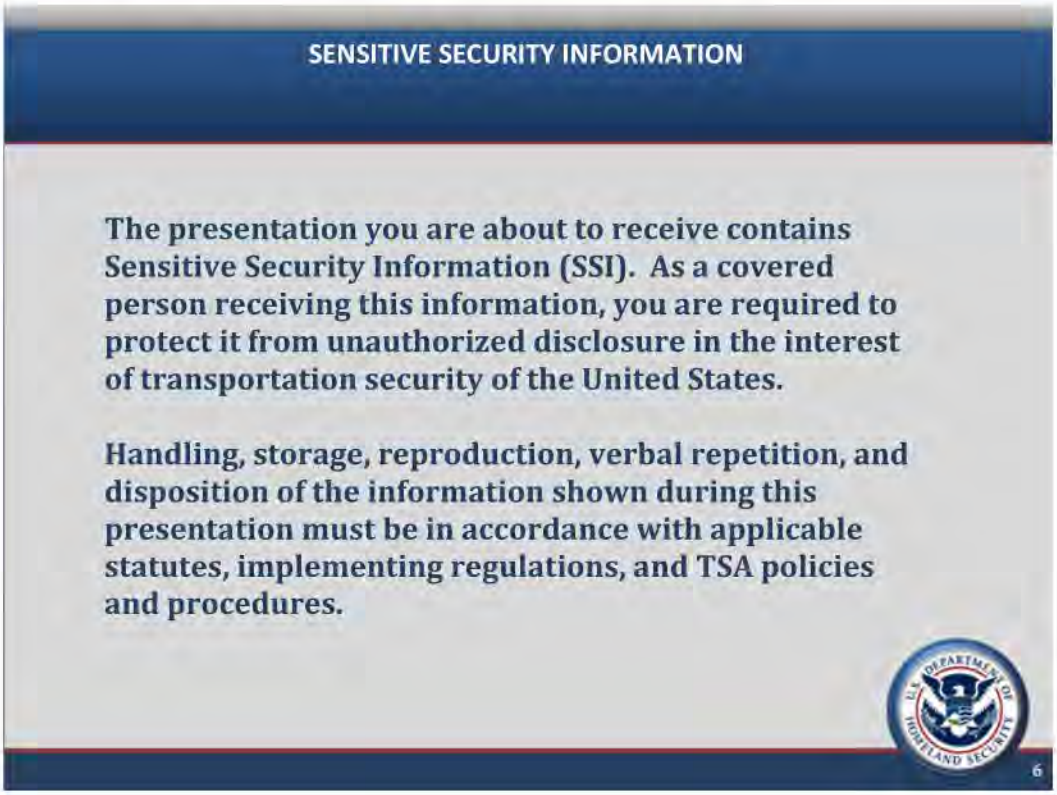
Table 1: SSI Marking Guidance for Records & Media

Type of Record	Marking
Emails	No header or footer should be present since SSI is not authorized in the body of emails; attachments containing SSI that are sent through email must comply with the SSI marking guidance for that record type and the encryption requirement (see subsection 5.3.3 *Methods for Applying Encryption to SSI*)
Documents (e.g., Word or Adobe® PDF)	Use of SSI Cover Sheet (DHS Form 11054) encouraged; use header and footer on every page and on any covers
Presentations (e.g., PowerPoint)	Use of SSI Cover Sheet (DHS Form 11054) encouraged; use both header and footer on the first and last slides; use header only on all other slides (see subsection 4.2 *SSI in Presentations and Briefings*)
Spreadsheets (e.g., Excel)	Use of SSI Cover Sheet (DHS Form 11054) encouraged; use header on every page; use footer, or a picture image of the footer, on every page if possible. If not possible, use footer at the end of the spreadsheet
Databases (e.g., Access)	Output reports for databases producing SSI material must comply with the SSI marking guidance for "Documents"
Messaging Systems (e.g., Communicator)	No SSI is authorized in the body of a chat session; attachments containing SSI sent through chat must comply with the SSI marking guidance for that record type and the encryption requirement (see subsection 5.3.3 *Methods for Applying Encryption to SSI*)
Screen Images	Use marking guidance for the type of record the image is being placed in
Photographs	Place the header and footer wherever they can be readily seen or apply the header using labels or a permanent marker
Charts, Maps, and Drawings	Place the header and footer wherever they can be readily seen
Video and Audio Recordings	Apply header and footer to each side of every reel and storage container; if practical, record protection requirements audibly (see subsection 4.2 *SSI in Presentations and Briefings*) and/or show header and footer visually at the beginning and end of the recording
CDs, DVDs, and Diskettes	Apply header using labels or a permanent marker; and Apply header and footer on outside jewel case, jacket or sleeve
Mobile Electronic Media (e.g., USB Flash Drives)	No external marking, *but personnel must use a TSA-approved/provided encrypted media;* mark all records containing SSI as annotated in this table for the appropriate type of record

4.2 SSI in Presentations and Briefings

In addition to following the presentation marking requirements (see subsection 4.1 *Marking Records & Media Containing SSI*), if a presentation or briefing contains SSI, the following language must either (1) appear on the first slide under the cover slide, or (2) be read to the audience at the start of the briefing:

> "The presentation you are about to receive contains Sensitive Security Information (SSI). As a covered person receiving this information, you are required to protect it from unauthorized disclosure in the interest of transportation security of the United States.
>
> Handling, storage, reproduction, verbal repetition, and disposition of the information shown during this presentation must be in accordance with applicable statutes, implementing regulations, and TSA policies and procedures."[10]



[10] **Note:** When providing the presentation or briefing to non-DHS employees, remove the reference to "TSA policies and procedures" as other covered persons outside of the DHS network are not required to follow TSA policies and procedures for safeguarding SSI.

5.0 Safeguarding SSI

SSI may be disclosed to *covered persons* who have a *need to know* the information (*See also* subsection 6.1 *Determining Covered Persons with a Need to Know*). Covered persons must *protect* SSI by ensuring it is disclosed only in a secure manner, achieving an effective balance between information sharing and information protection. This section of the Handbook provides ways to safely share, yet reasonably protect, SSI. Any technology not explicitly covered below must receive Chief Information Security Officer (CISO) and SSI Program office approval prior to security implementation.

5.1 General Protection of SSI

Personnel who possess records containing SSI are responsible for ensuring those records are protected at all times to prevent disclosure to non-covered persons or to covered persons who do not have a need to know. See TSA MD 1400.3, *Information Technology Security*, and Attachment 1, *TSA Information Assurance Handbook*, for specific information-security policies and guidelines for TSA computer networks, systems, and equipment. The TSA IT Security Policy applies to all TSA personnel and all TSA information systems that collect, generate, process, store, display, transmit, or receive TSA data, including prototype and telecommunications systems.

- When not under direct physical control, lock up the record containing SSI, including records stored on TSA-owned portable devices such as USB flash drives, CDs, or other portable devices, in a desk drawer, cabinet, or office. The *TSA Information Assurance Handbook* requires logging off from or locking unattended computers. This can be done by simultaneously hitting the Ctrl + Alt + Delete keys or simultaneously hitting the Windows® key and "L" key.
- Destroy SSI when it is no longer needed. (*See also* subsection 7.0 *Destruction of SSI*).
- To transport or transmit SSI, use of the SSI Cover Sheet (DHS Form 11054) is encouraged.

5.2 Protecting SSI in Transmission & Storage

Personnel must ensure proper protection of information created, stored or transmitted to limit access to covered persons with a need to know. The following subsections serve as guidance for the protection of information through a variety of media, including storage of data on networked storage (e.g., Local Area Network (LAN) drives), collaborative applications (e.g., iShare and SharePoint) and local hard drives. For more information, contact the SSI Program office at SSI@tsa.dhs.gov.

5.2.1 The Internet

Personnel shall not, under any circumstances, post records containing SSI to a publicly accessible Internet site[11] that is not authenticated and restricted to those with a need to know, even if the record is encrypted (*see also* subsection 3.5 *Requesting an SSI Assessment or SSI Review from the SSI Program*). Before posting anything on the publicly accessible TSA Internet website or any other Internet website, personnel must evaluate whether the content could *possibly* constitute SSI. Content is not limited to documents, but could also be in the form of photos, video, audio recordings, etc. All personnel are

[11] Secure Internet sites approved for handling SSI are addressed in section 12.0 *Protection Requirements for SSI Systems & Other Secure Sites*

obligated to protect SSI from posting to the Internet, whether the posting is made at work or off-duty. ***Note:*** *Internet posts can take many forms. SSI is frequently found improperly posted on social networking and job-hunting sites. SSI shall not be posted to these, or any other, types of sites.*

Before TSA personnel post any record (a document, chart, graphic, video or other published work) to the publicly accessible TSA Internet website or any other Internet website, they must certify that the record contains no SSI by following the steps below. ***Note:*** *Following this process does not remove the employee's responsibility to obtain supervisory approval prior to posting content related to work to a publicly accessible website.*

- If the record could possibly contain SSI, personnel must send the record to either their designated SSI Coordinator or to the SSI Program office for an SSI Assessment (*see also* subsection 3.5 *Requesting an SSI Assessment or SSI Review from the SSI Program*).
- After the SSI Coordinator or SSI Program office personnel determine the record contains **no SSI**, the record may be posted on the Internet.
- If the record *does* contain SSI, the requesting TSA personnel—with the assistance of their SSI Coordinator or the SSI Program office—must have the record edited to remove the SSI or have an Authorized Redactor redact the SSI before posting the record.
- Each office posting to the Internet must retain records, subject to their office's records retention schedule, of the SSI Assessment conducted and the finding that the record contained **no SSI.**
- ***Best Practice:*** *Sometimes, after an electronic record is edited to remove SSI, SSI content remains in the metadata[12] of the record. If SSI is removed from a record, a simple way of ensuring the metadata does not remain is by ensuring all track changes are resolved and removed, copying all the non-SSI content, and pasting the non-SSI content into a blank (new) record.*

5.2.2 TSA Shared Network Resources: Shared Drives, Systems & TSA Intranet

SSI protection requirements for both TSA shared drives and Intranet are the same. These collaborative systems are on a restricted or closed computer network. Although portions of the TSA Intranet sometimes look like Internet sites, the TSA Intranet is not open to everyone. Still, a large community of people can access both TSA shared drives and Intranet sites if they are granted permission.

SSI may be stored without encryption on TSA shared network drives and folders and within the various TSA Intranet and SharePoint (e.g. iShare) sites as long as access is limited to persons with a determined need to know and the records are properly marked (see Table 2: *SSI Posting Guidance for TSA Collaborative Applications (e.g. iShare)*). Owners and administrators must periodically review the security settings and user permissions for these drives, folders, and sites that contain SSI to verify access is limited to only those covered persons with a need to know and must promptly remove access for those individuals who no longer have a need to know the SSI.

Some systems[13] within TSA shared drives or within the TSA Intranet may contain SSI. Information System Security Officers (ISSOs) for IT systems must complete an SSITA and, if the system contains SSI, they may also be required to complete an SSIIA (*see also* section 11.0 Determining *SSI Systems*).

[12] Electronically stored data that provides information about other data (e.g., track changes, author, creation, etc.).
[13] Use of term "systems" also includes databases.

Sharing SSI through collaborative applications such as Microsoft's SharePoint (e.g., TSA iShare) is permitted so long as access is limited to covered persons with a need to know. TSA has implemented color-coded layers within the TSA iShare to assist in the identification of areas where SSI may be posted. Posting of SSI must follow the procedures for the corresponding color-coded layers, as defined below. In addition to these requirements, personnel must check and adhere to Terms of Use Agreements for each page/team site.

Table 2: SSI Posting Guidance for TSA Collaborative Applications (e.g. iShare)

Access Layer	Who Has Access?	Okay to Post SSI?
BLUE (TSA Portal)	All TSA personnel and many TSA contractors Some parts of the Blue layer are open to all DHS personnel Search engines must not provide visibility to approved SSI locations within the Blue Layer	**No** SSI on blue layer, with the following exceptions: • TSApedia and Blogs (currently) • IdeaFactory **NOTE:** SSI *must* still be marked in the exception areas – these areas are not open to all DHS personnel[14]
GREEN (Team Sites)	Persons granted permission by the site administrator; some green layers have open access to large audiences Site administrator must examine the site's permissions periodically to ensure everyone with access to the site has a need to know the information contained therein Search engines must not provide visibility to SSI on the Green Layer to individuals without explicit access	Yes, with *restricted permission to the people with a determined need to know* SSI Program policies do not require additional encryption as long as the content is limited to people with a need to know and the record is properly marked Terms of Use Agreements or site administrators may require further protections
RED (My Site)	*Shared Documents:* All TSA personnel and many TSA contractors can access these documents	**NO**
	Personal Documents: Only the individual and other personnel to whom the individual has specifically granted access Search engines must not provide visibility to SSI on the Red Layer to individuals without explicit access	Yes, as long as only those with a need to know the information have access and the record is properly marked

For information on how to protect SSI through other SSI Systems, such as TSA WebBoards, and other secure sites, see subsection 12.0 *Protection Requirements for SSI Systems & Other Secure Sites.*

[14] Offices seeking exceptions to place SSI on the Blue layer of iShare should seek approval in writing from the Deputy Administrator through the SSI Program office.

5.2.3 Encrypting SSI in Transmission

Records containing SSI must be encrypted within all email, even within DHS, as well as during other types of electronic transmission traveling outside the DHS enclave. SSI must never be placed in the body of an email and must be encrypted separately, unless an email encryption method is available. Additionally, SSI must be encrypted in other forms of electronic transmission as detailed in the *TSA Information Assurance Handbook*.

Images or video which may contain SSI may be transmitted within the mobile device security sandbox (e.g., Good software) for operational needs. *For example, an image of a suspect item taken within the Good software and transmitted to a TSS-E for evaluation is authorized.*

TSA personnel shall treat any official images or video as SSI and begin to protect them with SSI markings and encryption in transmission as soon as operationally viable. SSI markings may be removed and other protection requirements cease only once the image or video has been assessed to not contain SSI. For more information, see Section 3.3, *Conducting SSI Assessments*.

Note: *Other methods of encrypting a record for transmission may be established by the system owner (SO) in coordination with the TSA Office of Information Technology (OIT) and the SSI Program.* For more guidance on the use of passwords, see subsection 5.3 *Passwords*. Encryption methodologies must be consistent with Technical Standard TS-002, *Encryption*.

5.2.4 Electronic Devices

SSI may be stored on TSA-owned devices without encryption as long as the device itself is protected with a password that meets DHS and TSA IT security requirements. All TSA data must be encrypted when stored on government furnished equipment (GFE), such as removable media (e.g., disks or CDs) or portable drives (e.g., USB flash drives) (*see also* subsection 5.3 *Passwords*). SSI may not be stored outside of the Good container on iOS (i.e., iPhone) devices.

Personnel must not open, view, process, download or store SSI on non-GFE, including computers, cell phones, Personal Data Assistants (PDAs), USB flash drives (thumb drives), MP3 players, or portable hard drives that have not been approved by TSA OIT. These prohibited devices are not approved for use on TSA equipment. *See also* TSA MD 1400.3, *Information Technology Security*, its associated Attachment 1, *TSA Information Assurance Handbook*, and the DHS Sensitive Security Systems Policy Documents (4300A).

Per the DHS 4300A, version 8.0, 5.4.6.i, "Auto-forwarding or redirecting of DHS email to addresses outside of the .gov or .mil domain is prohibited and must not be used. Users may manually forward individual messages after determining that the risk or consequence is low." Additionally, personnel must not forward emails containing SSI to personal email addresses (e.g., Hotmail, Yahoo).

SSI must be removed from all electronic media before resale, disposal, or reuse outside of the agency. For more information, see Section 7.0, *Destruction of SSI*.

Note: *For information on traveling with TSA-owned equipment that contains SSI, see subsection 5.2.10 Removing SSI from the Workplace (Traveling with SSI). See also subsection 7.0 Destruction of SSI for more information on handling information on electronic devices.*

5.2.5 Scanners, Copiers & Printers

When scanning, copying, or printing records containing SSI, personnel must employ safeguards to protect the SSI and ensure it cannot be accessed or stolen by non-covered persons or covered persons who do not have a need to know. Reproducing SSI using these methods often places the data in shared locations that can be accessed by multiple individuals over a network or through direct, physical access if proper security measures are not implemented.

Personnel shall only process records containing SSI using TSA-owned, GFE in TSA facilities by covered persons with a need to know. However, 3rd party equipment, facilities, and services (e.g., Kinko's, FedEx, or Staples) may be used if purchased through the acquisition process in accordance with the Government Printing Office Simplified Purchase Agreement (SPA) program requirements.[15] TSA contractors scanning or reproducing SSI material in the performance of their contract shall use TSA-owned GFE or their respective contractor-owned equipment for processing SSI. Use of other 3rd party equipment shall require prior approval of the COTR. Processing SSI on non-GFE not approved for use by TSA OIT is prohibited.

For scanners, copiers, and printers, password-protection and data encryption are considered minimum requirements for SSI data at rest and in transit. The CISO shall provide procedures and instructions in cases where this functionality is not available. Passwords created to encrypt information and the encryption itself shall be compliant with Technical Standard TS-001, *Passwords* and Technical Standard TS-002, *Encryption*, respectively. *See also* subsection 7.0 *Destruction of SSI* for more information.

Personnel must conduct proper sanitization and disposition of media used to process SSI as it is critical to ensuring confidentiality. Printing, scanning, and copying devices typically contain persistent memory such as hard drives or internal flash memory to store data. TSA and DHS disposition requirements[16] prohibit this media from leaving the facility and require that it be destroyed on-site. All associated sanitization and disposition of media used to process SSI shall be consistent with the *TSA Information Assurance Handbook*, including section 3.10, *Media Sanitization*. *See also* Technical Standard TS-046, *IT Media Sanitization and Disposition*, NIST Special Publication 800-88 [Guidelines for Media Sanitization] for guidance on destruction of SSI on electronic media by using any of the designated methods, and DHS Sensitive Security Systems Policy Documents (4300A) for more information.

Note: *Exceptions to this policy may be approved by the SSI Program Chief on a case-by-case basis. Field requests for exceptions must be routed though the respective operational chain-of-command and TSA headquarters office to the SSI Program Chief as the approving authority.* TSA Form 1408, *IT Waiver/Exception Request* *with AO approval may be required if the policy exception is related to an Information Assurance policy requirement.*

[15] Through the SPA program, GPO issues agreements with third party document reproduction facilities on behalf of the requiring agency. The GPO also has their own printing facilities which may be used for sensitive material reproduction. Requests for processing SSI through GPO must be submitted to the Office of Acquisition.
[16] Refer to DHS Sensitive Security Systems Policy Documents (4300A), Section 4.13 for further detail.

5.2.6 Faxes

Personnel may send records containing SSI via fax as long as the recipient is a covered person with a need to know. Before sending the fax, personnel must (1) complete the SSI Fax Cover Sheet, (2) verify that the fax number of the covered person is correct and current, and (3) verify that either the recipient is standing by to receive the faxed record or that the fax machine is in a secure area accessible by only those with a need to know the SSI. *See also* subsection 5.2.5 *Scanners, Copiers, & Printers* for information on configuring, maintenance, or disposal of facsimile machines.

5.2.7 Telephone

Personnel may discuss SSI over the telephone as long as all persons present are covered persons with a need to know. Personnel must not discuss SSI if their conversation can be overheard by someone who is not a covered person or who does not have a need to know. Personnel must be cognizant of their surroundings when using a speakerphone.

Use of landline phones or the TSA-approved VOIP (Voice Over Internet Protocol) system (e.g., TSA Headquarters phone system) when discussing SSI is preferred. Personnel must not include SSI in voicemail messages. When using TSA-encrypted radios, walkie-talkies, or other mobile computing devices to discuss SSI, take precautions to discuss SSI sparingly and privately. Use of personal cell or cordless phones to discuss SSI is discouraged. For further information, consult Technical Standard TS-021, *General Telephony*.

5.2.8 Video Teleconferencing (VTC)

Personnel may discuss and/or display Sensitive Security Information (SSI) via TSA's video teleconferencing technology (VTC) as long as all participants are covered persons with a need to know the information. Personnel must not opt to have the call monitored by any non-TSA personnel servicing the VTC, and must suspend discussion and/or display of SSI during any period when a non-covered person is present (e.g., while a person is present providing technical support for the VTC session).

TSA VTC sessions may be recorded only when the recording is stored on a user-restricted TSA internal system (this is default for intra-TSA VTC), such that the information cannot be accessed by a person who does not have a need to know. Storage of SSI data from a VTC session on an externally-hosted system is prohibited. Organizers of VTC sessions should restrict access to intended invitees who have a need to know the information, and shall verify attendance during the conference to ensure that only covered persons with a need to know are present during the VTC session.

Adobe® Connect® is an externally-hosted system currently authorized for use for video teleconferencing within TSA. Presentations containing SSI may not be uploaded into Adobe® Connect®. During the use of externally-hosted VTC software, discussions which will contain SSI may only be held through a separate unmonitored teleconferencing line. If SSI is required to be shown during the presentation while using externally-hosted VTC systems, it may be done only through the use of "Share My Screen" (i.e., screen share) functionality (See image at right). Likewise, "Share Desktop" function is authorized for display of SSI through Microsoft® Communicator®.

5.2.9 Packaging & Delivering SSI

When personnel need to hand-deliver SSI, send it through the mail, or carry it from one location to another, they must follow the procedures below in order to minimize the risk of loss or improper disclosure. While packaging records containing SSI, personnel must ensure that the records are properly marked. *See also* subsection 4.1 *Marking Records & Media Containing SSI*.

Table 3: Guidance on Packaging SSI	
U.S. Mail (including U.S. authorized commercial delivery services such as FedEx, UPS, etc.) Interoffice Mail	1. Attach the SSI Cover Sheet, DHS Form 11054, to the records (encouraged but not required) 2. Use an opaque (cannot see through) envelope, wrapping, or carton 3. Do not mark the envelope or outside wrapping with the SSI header or footer, or any other indication of the contents' sensitivity 4. Address with an attention line containing the name and office of the intended recipient 5. For U.S. Mail, send by USPS First Class certified mail or another traceable delivery service requiring signature upon delivery
Hand-carrying (on-site)	1. Attach the SSI Cover Sheet, DHS Form 11054, to the records (encouraged but not required) 2. Do not leave SSI unattended or unlocked in the recipient's workspace
Hand-carrying (off-site)	1. Attach the SSI Cover Sheet, DHS Form 11054, to the records (encouraged but not required) 2. Place material in an opaque (cannot see through) envelope or case 3. Do not leave SSI unattended or unlocked in the recipient's workspace

When personnel must transfer large quantities of data, such as thousands of scanned images, and it is impractical to zip and encrypt the files or store the data on separate USB flash drives or CDs, the entire hard drive may need to be sent to the intended recipient. In the case of sending an entire hard drive or other physical media (i.e., electronic devices) containing SSI, personnel shall use the following procedures:

- Apply the SSI header and footer label on the exterior casing of the hard drive;
- Double-wrap the hard drive using tamper-resistant wrapping;
- Ship the hard drive using FedEx, UPS, or U.S. Mail (Certified) with a tracking number; and
- Use only drives that are TSA-approved encrypted hard drives; send the password separately.

Shipping of SSI to overseas offices is permitted only when approved by the Office of Global Strategies (OGS) or the office is serviced by a U.S. Embassy, Consulate, or military postal facility (i.e., APO/FPO). Where the overseas office is not serviced by a U.S. Embassy, Consulate, or military postal facility, the materials will be sent through OGS, the Department of State, Diplomatic Courier or TSA employee traveling on official business. *See also* subsection 5.2.10 *Removing SSI from the Workplace (Traveling with SSI).*

5.2.10 Removing SSI from the Workplace (Traveling with SSI)

Personnel must obtain permission from their supervisor before removing SSI from their workplace. Contract employees must obtain permission from their contracting officer technical representative (COTR) before removing SSI from the workplace. When SSI is removed from the workplace, protect it by maintaining positive physical control over the SSI or properly securing the SSI in a locked container so it is not accessible by non-covered persons or those who do not have a need to know the information.

Personnel shall only process electronic files containing SSI using TSA-approved devices (e.g., VPN-enabled TSA laptops). Personnel shall not use non-GFE (e.g., computers or other electronic devices) to process SSI (*see also* subsection 13.0 *SSI Policy Exceptions* for information regarding times of national emergency or exigent circumstances). Storing SSI on non-GFE devices is prohibited.

While traveling, personnel shall maintain positive physical control over the SSI and electronic devices[17] containing SSI whenever possible. If circumstances require SSI to be left unattended in a vehicle, the vehicle must be locked and the SSI material, or any container holding the material, must not be left in plain view. If circumstances require SSI to be left unattended at any time during travel (e.g., in a hotel room or at home), secure the SSI in a locked container (e.g., in hotel safe) to prevent unauthorized access to the SSI by others, including co-habitants, intruders, or hotel staff.

The guiding principle for securing SSI during travel is to take all reasonable steps necessary to protect SSI from access by non-covered persons or those without a need to know the information. For more information, see resource *Protecting SSI and Sensitive PII Away from the Workplace*.

[17] See also TSA MD 1400.3, *Information Technology Security*, its associated Attachment 1, *TSA Information Technology Security Handbook* for additional IT security requirements on removable media.

5.3 Passwords

Personnel must ensure proper protection of SSI created, stored, processed or transmitted to limit access to covered persons with a need to know. The following subsections serve as guidance for how to encrypt information using passwords.

5.3.1 Standard TSA Password

Personnel may use the Standard TSA Password when sharing SSI with covered persons who have a need to know and are within DHS. TSA's SSI Program office creates a new Standard TSA Password[18] on a 90-day cycle or in response to a password breach (see subsection 5.3.5 *Password Incidents*), and distributes the password to SSI Coordinators via email. SSI Coordinators then distribute this password to personnel within their area of responsibility who have a need to know the Standard TSA Password. For the current Standard TSA Password, personnel should contact their designated SSI Coordinator.

The SSI Program office provides SSI Coordinators with an application to access a historic Standard TSA Passwords list. SSI Coordinators can further share this application with personnel who have a need to know, and must periodically review and update the list of those who have access. Personnel must protect all historic password lists and applications as Sensitive Security Information. Personnel must not maintain their own personal or office list of historic Standard TSA Passwords nor print or further distribute such lists. Personnel must not use the password application to build a historic password list.

The SSI Program office maintains the Standard TSA Password primarily for sharing SSI. To lessen the administrative burden created by maintaining multiple standard passwords across TSA, the Standard TSA Password may also be used to protect other sensitive information within TSA, as necessary.

To disclose SSI to covered persons outside of DHS, personnel must not use the Standard TSA Password and must instead create their own password to protect the SSI in transmission (see subsection 5.3.2 *Creating Passwords to Encrypt SSI*). A password incident occurs when the Standard TSA Password is shared outside of DHS (see subsection 5.3.5 *Password Incidents*).

5.3.2 Creating Passwords to Encrypt SSI

Passwords must be consistent with Technical Standard TS-001, *Passwords*. When creating a password to encrypt records that contain SSI, personnel must follow these criteria:

- All passwords must:
  a. Be at least eight characters in length;
  b. Have at least one upper-case and one lower-case letter;
  c. Contain at least one number; base 10 digits (e.g., 0 through 9);
  d. Contain at least one symbol (e.g., *&^%$#!); and
  e. Not be a word in the dictionary or a portion of the file name
- Personnel may use the same password for multiple documents shared between the same sender and recipient.

[18] The Standard TSA Password is also known as the TSA National Password or the TSA SSI Password. For consistency and to reduce confusion, please use the term "Standard TSA Password."

5.3.3 Methods for Applying Encryption to SSI

The following table provides guidance on which types of electronic systems and devices require encryption when storing SSI:

Table 4: Encryption Standards for Various Media*

Type of Media	Encryption Required?
Email	Yes. Encrypt SSI in an attachment to the email. SSI is not authorized in the body of emails. Send the password in a separate email.
Shared Network Folders	No. Encryption is not required as long as the folder is restricted to those with a need to know.
Internet Sites	Posting SSI to the Internet (publicly-accessible sites) is strictly prohibited, even if it is encrypted, unless the site is authenticated and restricted to those with a need to know.
Intranet (including iShare) and other secure sites	No. Encryption is not required as long as access to the site is restricted to those with a need to know and the site is not searchable by individuals without access (*see also* Table 2*: SSI Posting Guidance for TSA Collaborative Applications (e.g. iShare)*).
Office Communicator	Yes. Encrypt SSI in an attachment to the Communicator message. SSI is not authorized in the body of Communicator messages.
Scanners	Yes. Use encryption when possible. When not possible, immediately delete any files in queue.
Fax	No.
Databases	No. Additional encryption is not required as long as the database has access restricted to covered persons with a need to know.
CDs, DVDs, and Diskettes	Yes. Whenever possible, encrypt all records that contain SSI.
Mobile Electronic Media (e.g., Removable Hard Drives, USB Flash Drives)	No. The device must be a TSA-approved encrypted media; the files do not need to be individually encrypted.

*This chart is intended to address encryption requirements. For further information on marking or safeguarding SSI on these systems or devices, see the relevant subsection.

The following methods may be used to encrypt records. Other encryption methods shall adhere to the requirements of

MS Office 2010 Products[19]

To encrypt records in MS Word (documents), Excel (spreadsheets), and PowerPoint (briefings and presentations) 2007, follow these steps:

Step 1. Select File > Info > Permissions

Step 2. Click on **Protect Document**.

Step 3. Select on **Encrypt with Password**.

Step 4. A dialog box appears. Type a password in the dialog box (see subsection 5.3.2 *Creating Passwords to Encrypt SSI*), and click **OK**.

Step 5. Retype the password in the next dialog box that appears, then click **OK**.

Step 6. **SAVE** the document to ensure the encryption is complete.

Adobe® Acrobat® 11 Pro

To encrypt records in Adobe® Acrobat® 11 document, follow these steps:

Step 1. Select File > Properties > Security

Step 2. On the drop-down list, select on "**Password Security**" (the second item in the drop-down list).

Step 3. In the next dialog box, click in the small box to the left of the line, "**Require a password to open the document**," as shown below:

Step 5. Click on and type in a password (see subsection 5.3.2 *Creating Passwords to Encrypt SSI*) in the box next to "**Document Open Password**," and click **OK**.
(***NOTE:*** *The employee may also restrict the editing and printing of the document by clicking in the appropriate box.)*

Step 6. In the next dialog box, confirm the "Document Open Password" by typing it again, then click **OK**.

Step 7. **SAVE** the document to ensure the encryption is complete.

[19] Excluding MS Publisher 2007.

WinZip

WinZip can serve as a catch-all program to encrypt other types of files aside from Microsoft Office and Adobe® files, such as photos or videos (e.g., jpeg, wave, avi file formats). To encrypt other records using WinZip, follow these steps:

Encrypting Files with WinZip 17

Step 1. Click on the **Encrypt** lock icon 

at the top of the screen. A dialog box stating "You should be aware of the advantages and disadvantages of the various encryption methods before using the feature. Please click on Help for more information, particularly if this is the first time you are using encryption." If so, click on **OK**.

Step 2. In the next dialog box, type in a password (see subsection 5.3.2 *Creating Passwords to Encrypt SSI*) in the box under "**Enter Password**."

Step 3. Re-type password in the box under "**Re-enter password (for confirmation),"** select an encryption method; SSI Program office recommends "Default – 256-bit AES encryption," then click on **OK.** An action box may appear showing the files being encrypted which closes when the encryption is complete.

Encrypting Files with WinZip 18.5

From WinZip ribbon interface

Step 1. Click on **START** -> **ALL PROGRAMS** -> **WinZip**

Step 2. Select the **Encrypt** button in the **Create/Share** TAB (Note: No pop-up will come up)

Step 3. Select ***From PC or Cloud*** button in the **Create/Share** TAB

Step 4. Find and select (highlight) the document you want to zip

Step 5. Enter a password when the **Encrypt** dialog displays

Step 6. Save the Zip file

From Folder Window

Step 1. Right click on the document you would like to zip

Step 2. Click **WinZip** -> **Add to Zip file**

Step 3. Check the box for **Encrypt Added files**

Step 4. Enter a password when the **Encrypt** dialog displays

Step 5. Save the Zip file

Encrypting data in an existing Zip file

Step 1. Right click on the Zip file in a folder window

Step 2. Choose **WinZip**

Step 3. Click **Encrypt**

5.3.4 Transmitting SSI Passwords

The Standard TSA Password or other password may be shared (*see also* subsection 5.3.2 *Creating Passwords to Encrypt SSI*) in person, over the telephone, in a voicemail message, or in an email with no subject line or with a non-descript subject line. This email *must not* contain the record the employee is trying to protect.

Personnel must not forward the Standard TSA Password outside of DHS (see subsection 5.3.1 *Standard TSA Password*). ***Best Practice:*** *If the document will likely get forwarded beyond DHS to other covered persons with a need to know the information, create a separate password to help reduce the number of SSI Password incidents.*

5.3.5 SSI Password Incidents

An SSI password incident occurs when either (1) a password created to encrypt SSI is inappropriately shared with covered persons in a manner not in accordance with this Handbook (see subsection 5.3.4 *Transmitting SSI Passwords*); or (2) the Standard TSA Password is shared with persons outside of DHS. *See also* subsection 10.3 *Password Incident Response & Resolution*.

6.0 Disclosure of SSI

According to the SSI Regulation, records containing SSI are not available for public inspection or copying. As such, TSA does not release records containing SSI to covered or non-covered persons who do not have a need to know. The SSI Regulation does, however, provide for authorized disclosure of SSI to the groups and persons described below.

6.1 Determining Covered Persons with a Need to Know

Generally, a *covered person* is an individual or entity who has transportation security or transportation security-related responsibilities to include, but not limited to, (1) anyone who is permanently or temporarily assigned, attached, detailed to, employed by, or under contract with DHS, (2) regulated parties, Federal, State, Local and tribal government employees, contractors, and grantees, as well as TSA stakeholders and industry partners; (3) Committees of Congress; (4) other persons with a need to know as defined in § 1520.11; and (5) persons receiving SSI pursuant to other conditional disclosures. ***Note:*** *Just because an individual is a covered person does not mean they also have a need to know. Need to know determinations must be made on a case by case basis.* For a complete listing of covered persons or persons with a need to know, see the SSI Regulation at § 1520.7.

The SSI Program office provides additional guidance as to who is a covered person with a need to know:

- **Contractors:** A DHS or TSA contractor automatically becomes a covered person for the purposes of performing their contract starting *on the effective date* of the contract. A contractor will always be a covered person responsible for protecting SSI in accordance with the SSI Regulation, even after the termination or expiration of their contract. The contracting representative is responsible for ensuring all contractors complete required SSI training. After the performance period of the contract, a contractor no longer has a need to know SSI unless they fit into another category of covered person.
- **Subcontractors:** A subcontractor becomes a covered person for the purposes of performing their contract by virtue of the prime contractor's relationship with DHS or TSA. They may access SSI and are responsible for appropriately safeguarding any SSI in their possession. A subcontractor will always be a covered person responsible for protecting SSI in accordance with the SSI Regulation, even after the termination or expiration of their contract. The contracting representative is responsible for ensuring all sub-contractors complete required SSI training. After the performance period of the contract, a subcontractor no longer has a need to know SSI unless they fit into another category of covered person.
- **Foreign nationals:** A foreign national becomes a covered person if they fit into one of the categories of covered persons or persons with a need to know. Permission to disclose SSI to foreign nationals who are covered persons need not be coordinated through the SSI Program office.
- **Foreign governments:** There is an official information sharing security process for determining whether information may be disclosed to foreign governments. Per TSA MD 2810.1, *SSI Program*, the Office of Global Strategies (OGS) has the delegated authority to determine appropriate sharing of SSI. Any disclosure of SSI to foreign governments must be coordinated through the OGS, as it maintains delegated authority to authorize the disclosure of SSI to select foreign governments and select foreign entities (e.g., foreign airports and regional/multilateral aviation security organizations) determined to have a need to know the information. OGS

shares tracking and other information related to its SSI disclosures with the SSI Program office, in accordance with mutually agreed procedures.

- **Foreign and domestic intelligence partners:** Foreign and domestic intelligence partners who are already authorized recipients of classified national security information may receive access to SSI contained within intelligence products inherent to the nature of the partnership in the interest of transportation security.
- **Foreign air carriers:** Foreign air carriers regulated by 49 C.F.R. Part 1546 are covered persons even when owned by a foreign government and may access SSI for which they have a need to know.
- **Personal representatives:** A TSA employee may designate an advisor to serve as his/her personal representative consistent with TSA policy. Under the SSI Regulation, personal representatives are "covered persons" for purposes of access to SSI and may receive SSI when they have the requisite "need to know." *See* 49 C.F.R. §§ 1520.7(k), 1520.11(a)(4), and 1520.11(a)(5). Therefore, the personal representative must abide by the TSA and SSI requirements for personal representatives, including signing a non-disclosure agreement. For more information, see Section 6.3, *Disclosure of SSI to AFGE and Personal Representatives*.

See also Appendix 3: *Determining Need to Know Flow Chart,* to determine whether an individual is a covered person with a legitimate need to know the SSI. For further guidance, consult the SSI Program office at SSI@tsa.dhs.gov.

6.2 Non-Disclosure Agreements

The SSI Program office does not make a practice of determining *when* a Non-Disclosure Agreement (NDA) should be administered to covered persons, appropriately leaving that responsibility to the program office/covered person disclosing the SSI. The following guidance on NDAs is provided to aid personnel in determining whether an NDA is appropriate for each individual situation. Personnel who have determined that use of an NDA is appropriate must use DHS Form 11000-6, *Department of Homeland Security Non-Disclosure Agreement*, or another equivalent document approved by Office of Chief Counsel.

While the SSI Regulation does not speak to requirements for signing NDAs, they are a tool used by DHS and TSA to ensure that covered persons receiving sensitive information understand their responsibilities to protect that information.[20] NDAs should be executed prior to the disclosure of SSI and they shall only be used to disclose information with covered persons who have a need to know the information. The signing of an NDA does not allow disclosing of SSI with non-covered persons.

It is good practice when addressing a group of covered persons who do not routinely handle SSI to provide them with the SSI Program office's best practices guide. The NDA is an additional measure the covered person disclosing the information may want to consider. Responsibility for ensuring a covered person receiving SSI understands the responsibilities entailed rests with the party disclosing the

[20] As examples, OCC may require NDAs be signed in certain litigation access procedures and other offices have developed internal policies requiring NDAs be signed when providing SSI to stakeholders and contractors; Acquisition, when providing some contractors with SSI, requires NDAs be signed and maintained by the COTR; and some TSA systems designed for stakeholder use contain NDA language in their terms of use.

information. The SSI Program office generally advises those inquiring about NDAs to err on the side of caution by executing an NDA if the need is not clear.

6.3 Disclosure of SSI to AFGE and Personal Representatives

On June 29, 2011, the Federal Labor Relations Authority (FLRA) certified the American Federation of Government Employees (AFGE) as the exclusive representative of bargaining unit employees at the Transportation Security Administration (TSA).[21] Consistent with this certification, made under the TSA Administrator's February 4, 2011, Determination on Transportation Security Officers and Collective Bargaining[22] and AFGE's status as the union representative under the December 29, 2014, Determination on Transportation Security Officers and Collective Bargaining, and as explained herein, AFGE holds a status as a covered person under 49 C.F.R. Part 1520.

- AFGE as a Covered Person: The SSI Regulation does not explicitly address either a union's status as a "covered person," for the purposes of collective bargaining, or a union's "need to know" SSI. However, section 1520.7(k) is applicable to "[e]ach person employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and including a person formerly in such position." Therefore, TSA determines that AFGE, as the certified exclusive representative of bargaining unit employees and acting in the collective interests of bargaining unit employees under the Determination, is a covered person under section 1520.7(k). TSA authorizes the disclosure of SSI to AFGE contingent upon the specific conditions of access and terms for protection of SSI detailed below.

- AFGE Representatives Serving as Personal Representatives: A TSA employee may designate an AFGE representative to serve as his/her personal representative consistent with TSA policy and § IV.A.4 of the Determination. When serving as a personal representative, the AFGE representative is serving in his/her personal capacity and not in his/her capacity as an AFGE representative. Under the SSI Regulation, personal representatives are "covered persons" for purposes of access to SSI and may receive SSI when they have the requisite "need to know." *See* 49 C.F.R. §§ 1520.7(k), 1520.11(a)(4), and 1520.11(a)(5). Therefore, the AFGE representative serving as a personal representative must abide by the TSA and SSI requirements for personal representatives, including signing a non-disclosure agreement.

TSA has the regulatory authority, at 49 C.F.R. § 1520.11(c), to "*make an individual's access to the SSI contingent upon satisfactory completion of …other procedures and requirements for safeguarding SSI that are satisfactory to TSA*…." Pursuant to its authority under 49 C.F.R. § 1520.11(c), TSA has determined that, under the conditions stated below, AFGE may receive SSI when AFGE has the requisite "need to know" to perform its responsibilities under § IV.C.1.c of the Determination.

---

[21] Bargaining unit employees are full and part-time non-supervisory personnel carrying out screening functions under 49 U.S.C. § 44901, as that term is used in ATSA, § 111(d); specifically, Transportation Security Officers, Lead Transportation Security Officers, Master Transportation Security Officers (which include Behavior Detection Officers, Security Training Instructors, and Equipment Maintenance Technicians), and Expert Transportation Security Officers (which include Behavior Detection Officers, Security Training Instructors, and Equipment Maintenance Technicians).

[22] The Determination, among other things, provides the purposes for which the exclusive representative of bargaining unit employees, AFGE, may receive SSI.

To receive such information, AFGE must abide by the following conditions:

(1) AFGE agrees not to disclose SSI to any other person or entity outside of AFGE or TSA without the expressed written permission of TSA, irrespective of whether that person or entity is a covered person under the SSI Regulation;

(2) AFGE recognizes and understands that every AFGE employee, AFGE contractor, and AFGE representative does not have the "need to know" required to receive SSI by virtue of his/her employment or affiliation with AFGE. AFGE employees, AFGE contractors, and AFGE representatives will only share SSI with other AFGE employees, AFGE contractors, and AFGE representatives who have the requisite "need to know" in that specific matter in order to receive the relevant SSI;

(3) AFGE understands that it is a "covered person" as defined in 49 C.F.R. § 1520.7 and is required to comply with the safeguarding and handling provisions of 49 C.F.R. Part 1520;

(4) AFGE will adhere to TSA's *SSI Quick Reference Guide for DHS Employees and Contractors*, which contains instructions for the proper handling and storing of SSI;

(5) AFGE, in consultation with TSA, will train all of its employees, representatives and contractors who are or may be working with TSA employees on the requirements of this Contingent Disclosure and their obligations regarding SSI; and

(6) AFGE will submit requests for access to SSI for the purposes defined in § IV.C.1.c of the Determination to Labor Management Relations to TSAPartnership@tsa.dhs.gov. Labor Management Relations, in conjunction with relevant TSA program offices, will determine whether AFGE has the requisite "need to know" to receive the requested SSI on a case-by-case basis.

The identified conditions are intended to safeguard SSI shared with AFGE against unauthorized disclosure, and failure to meet the conditions may result in civil penalty or other enforcement or corrective by DHS, as authorized by 49 C.F.R. § 1520.17.

6.4 Congress and the Government Accountability Office (GAO)

Disclosures to Congress and GAO are covered in the SSI Regulation at § 1520.15, *SSI disclosed by TSA or the Coast Guard*. Per § 1520.15(c), records containing SSI may be disclosed to:

- Committees of Congress; and
- Comptroller General of the GAO or to any authorized representative of the Comptroller General.

Any disclosure of SSI to Congress must be coordinated through the Office of Legislative Affairs (OLA). TSA has interpreted SSI statutory and regulatory provisions to require disclosure to the chairperson of a committee or subcommittee of Congress authorized to have the information upon request.

Per TSA MD 2810.1, *SSI Program*, the Assistant Administrator (AA) of OLA has the authority to disclose SSI to a ranking member of an authorized committee or subcommittee of Congress.
The AA for OLA is responsible for ensuring that any disclosure of SSI to a ranking member of an authorized committee or subcommittee is conducted using the instructions available below:

- Determining the need for and authorizing the disclosure of SSI to a ranking member of any committee or subcommittee of the United States House of Representatives or the United States Senate authorized to have the information, upon a determination that the disclosure is not detrimental to transportation security, in accordance with 49 C.F.R. § 1520.15(e), while taking special care to ensure that recipients of SSI fully comply with restrictions, procedural safeguards, and limitations on further dissemination, in accordance with 49 C.F.R. Part 1520. This determination authority may not be further delegated beyond the Assistant Administrator for Legislative Affairs. The determination and authorization shall include:
    a. Coordinating with the program office/owner of the records being considered for release to a ranking member of a congressional committee or subcommittee and maintaining an auditable record of this coordination.
    b. Reporting to the SSI Program office in a timely manner, by means of a written determination memorandum as approved by the SSI Program office, the SSI that was disclosed and to whom it was disclosed.
    c. Limiting SSI disclosed under this section to the minimum amount necessary to allow ranking members of congressional committees or subcommittees to effectively conduct their congressional oversight functions.

Finally, other Members of Congress, in their individual capacity, are not considered employees of the Federal Government and the SSI regulation does not explicitly authorize the sharing of SSI with these Members.

6.5 Freedom of Information Act (FOIA) Requests

When the public wants to view government-held information about transportation security, they may request the information under FOIA. Records containing SSI may be released only *after* any SSI has been properly redacted from the record. FOIA requests that may involve SSI are handled as follows:

- FOIA requests are routed to the TSA FOIA Office for processing;
- The FOIA Office gathers responsive records and determines if the records *may* contain SSI;
- The FOIA Office forwards records that may contain SSI to the SSI Program office for review;
- The SSI Program office identifies any SSI in the records received from the FOIA Office and prepares a visually redacted version of the record; and
- The visually redacted version is sent to the FOIA Office for further processing and, before the responsive records are sent to the requester, the FOIA Office redacts the SSI identified by the SSI Program office in accordance with TSA MD 1400.17, *Document Redaction*.

6.6 State Open Records Requests

Similar to Freedom of Information Act (FOIA) requests, many state laws (e.g., "Sunshine" laws) provide citizens the right to access government records. Certain exemptions may apply to these requests such as information that is confidential by law, either constitutional, statutory, or by judicial decision. While laws vary by state, 49 C.F.R. § 1520.9(a)(3) requires that covered persons "*Refer requests by other persons for SSI to TSA*". This requirement for referral includes requests for access to SSI made under State, local, or tribal public information and related laws. SSI falls under the SSI Federal Regulation,

which preempts conflicting State, local, and tribal law. Processing requests within TSA should be handled as follows:

- Requests for TSA's own records made through State Open Records requests must be referred to TSA FOIA (FOIA.TSA@dhs.gov).
- Requests for records belonging to the state or airport authority should be submitted for full SSI Review to the SSI Program.
- Requests may be submitted by either TSA Field Counsel or a local SSI Coordinator using the on-line SSI Review Request tool.
- Requests for SSI Assessments of video may be completed by Certified SSI Coordinators. ***Note:*** *SSI Assessment requests of video for a contentious incident should be sent directly to the SSI Program at Headquarters.*

6.7 Enforcement Proceedings

As defined in § 1520.11(a)(5), records containing SSI may be disclosed to persons in judicial or administrative enforcement proceeding when access to the SSI is necessary for the persons to prepare a response to allegations in a legal enforcement and/or personnel action proceeding.

Before granting access to SSI in an enforcement proceeding, TSA may require persons to undergo a background check with favorable results. Such disclosures must be handled by the Office of Chief Counsel and the SSI Program office as defined in TSA MD 2810.1, *SSI Program*, (*see also* subsection 6.2 *Non-Disclosure Agreements*).

6.8 Other Conditional Disclosures

Specific records containing SSI may be conditionally disclosed to a non-covered person upon a written determination signed by the TSA Administrator or designee that disclosure would not be detrimental to transportation security. TSA may place limitations or restrictions on the disclosure and describe those limitations in the written determination, known as a 15(e) memo.[23] The requester of a 15(e) memo must supply the SSI Program office with the following information to develop the 15(e):

- The specific SSI proposed for disclosure;
- The background and purpose of the disclosure;
- Any proposed restrictions or limitations regarding the disclosure; and
- The benefit disclosure will have to transportation security.

Persons granted conditional disclosure by virtue of a 15(e) memo become covered persons under § 1520.7 of the SSI Regulation and have a duty to protect SSI under § 1520.9.

[23] Section 1520.15(e) of the SSI Regulation grants the TSA Administrator the authority to make these written determinations. The Administrator's authority to make these 15(e) determinations is primarily delegated to the SSI Program Chief in TSA MD 2810.1, *SSI Program*.

7.0 Destruction of SSI

Subject to applicable records retention laws, schedules, and directives (see TSA MD 200.7, *Records Management Program*), records containing SSI must be destroyed to prevent recognition or reconstruction using the following procedures:

Destruction of Paper SSI

- Dispose in an SSI bin, if available;
- Shred in a cross-cut shredder so particles do not exceed 1 ½" by ¼";[24] or
- If no shredder is available, manually cut or tear the document so the pieces are ½-inch on a side or smaller and, after cutting or tearing the document, mix the material with other wastepaper material

Destruction of Optical Media (CDs, DVDs, Disks, etc.)

- Use one of the following authorized methods of destruction: shredding, incinerating, or disintegrating, in accordance with *TSA Information Assurance Handbook*, Section 3.10 *Media Protection* and Technical Standard TS-046, *IT Media Sanitization and Disposition*.

Destruction of Electronic Media (USB Flash Drives, Hard Drives, Copy Machines, Scanners, etc.)

- SSI must be removed from all electronic media before resale, disposal, or reuse outside of the agency.
- A determination of whether a copier drive, hard drive, USB flash drive, or scanner is cleared (wiped), purged, or destroyed is based on the security categorization level of information it contains and the security categorization of the system it falls within (*see also TSA Information Assurance Handbook*, Section 3.10 *Media Protection* and Technical Standard TS-046, *IT Media Sanitization and Disposition*, to determine if the information warrants clearing, purging, or physical destruction; *see also* Table 5: *NIST Specific Guidance on Destruction of Electronic Media* below for instructions on media destruction).

If destruction of SSI is completed by a document destruction vendor, either 1) the vendor employees must be vetted by TSA in accordance with § 1520.11(c) or 2) the SSI must be collected and destroyed under the direct supervision of a TSA employee using one of the methods authorized for the destruction of SSI. Upon destruction completion, the vendor must also provide TSA with a document signed by the vendor, or his or her authorized representative, and witnessed by the TSA employee who supervised the destruction, outlining how the SSI was destroyed.

Personnel must conduct proper sanitization and disposition of media used to process SSI as it is critical to ensuring confidentiality. Printing, scanning, and copying devices typically contain persistent memory such as hard drives or internal flash memory to store data. TSA and DHS disposition requirements[25]

[24] If destruction of SSI is completed by a vendor in bulk, the maximum acceptable size particles that vendors must conform to is 1 ½" by 5/8".

[25] Refer to DHS Sensitive Security Systems Policy Documents (4300A), Section 4.13 for further detail.

prohibit this media from leaving the facility and require that it be destroyed on-site. All associated sanitization and disposition of media used to process SSI shall be consistent with the *TSA Information Assurance Handbook*, including section 3.10, *Media Sanitization*. *See also* Technical Standard TS-046, *IT Media Sanitization and Disposition*, NIST Special Publication 800-88 [Guidelines for Media Sanitization] for guidance on destruction of SSI on electronic media by using any of the designated methods, and DHS Sensitive Security Systems Policy Documents (4300A) for more information.

8.0 SSI Training Programs

The SSI Program office currently offers three levels of SSI training programs.

Basic SSI Training: This SSI training for covered persons addresses the principles of identifying, marking, safeguarding, disclosing, and destroying SSI. Basic SSI training is required for all personnel within the first 60 days of employment with TSA. This training is also required annually for all personnel with an Online Learning Center (OLC) account. COTRs for TSA contractors and subcontractors without an OLC account are responsible for ensuring these contractors adhere to the requirements for basic SSI training. COTRs are also responsible for maintaining an auditable system to track training and training acknowledgements.

Advanced SSI Training: This training is delivered by the SSI Program office and provides a more detailed discussion on a number of high-interest topics. Completion of all Advanced SSI Training modules is required before an appointed SSI Coordinator or other covered person may take the SSI Certification Examination. The advanced SSI training modules may be taken individually or as a complete training program prior to taking the SSI Certification Examination.

At the end of the course, individuals take an SSI Certification examination. In order to receive SSI Certification, individuals must score at least 75% on each portion of the exam.

All appointed SSI Coordinators must complete Advanced SSI Training and pass the SSI Certification examination within one year of appointment. If an appointed SSI Coordinator does not pass the SSI Certification examination within one year of appointment or does not pass the SSI Certification examination after two attempts, the appointing official must appoint another TSA employee to serve as an SSI Coordinator. Once an SSI Coordinator becomes SSI Certified, the individual must complete annual CESSI Training, as outlined below, to maintain status as a Certified SSI Coordinator.

Covered persons other than SSI Coordinators may opt to take the Advanced SSI Training and Certification Examination. If they wish to maintain their SSI Certified status, they must also complete annual CESSI Training, as outlined below.

Continuing Education in SSI (CESSI) Training: Training issued by the SSI Program office and required of all SSI Certified individuals in order to maintain SSI Certified status. Individuals may either attend an annual CESSI course, or they can earn comparable SSI credit through various SSI related activities throughout the year. Sample activities include participation in the bi-monthly conference call, conducting SSI training or exercises at their office or airport, conducting awareness activities, etc. Also for CESSI credit, SSI Coordinators who have passed the SSI Certification examination may conduct the first-level of SSI Reviews prior to submitting a request for the additional levels of review to the SSI Program office.

9.0 SSI Awareness Programs

As part of TSA's SSI Awareness efforts, the SSI Program office leverages TSA's SSI Coordinator network to establish and maintain direct contact with all personnel. The SSI Program office uses a number of communication methods, to include Be On The Lookout (BOLO) notifications, bi-monthly SSI Coordinator teleconferences, and SSI Awareness Week activities. The SSI Program office also maintains the SSI iShare page to make its most critical documents and resources easily accessible by TSA personnel.

9.1 SSI Coordinators & SSI Area Coordinators

SSI Coordinators and SSI Area Coordinators (whose responsibilities are defined within TSA MD 2810.1, *SSI Program*) are a critical part of the SSI Program Awareness initiatives. SSI Coordinators are appointed by Assistant Administrators or their equivalents, Supervisory Air Marshals in Charge, and Federal Security Directors. See Appendix 2: *SSI Coordinator Designation Instructions* for more information on SSI Coordinator appointments.

An SSI Area Coordinator serves as the point of contact (POC) for SSI Coordinators in the field in geographic regions defined by the SSI Program Chief. The FAMS Area Coordinator is responsible for all FAMS field offices and resident agent offices. The SSI Program office uses the geographic areas defined by the Office of Security Operations as the delineation of areas of responsibility for the other SSI Area Coordinators, as follows:

SSI Eastern Area Coordinator – Areas 1-2 & 7
SSI Central Area Coordinator – Areas 3-4
SSI Western Area Coordinator – Areas 5-6

For more information on SSI Coordinator responsibilities, see TSA MD 2810.1, *SSI Program* (Section 5.C), Appendix 9: Instructions for New SSI Coordinators, and Appendix 10: Instructions for Certified SSI Coordinators.

9.2 SSI BOLOs

The SSI Program office uses BOLOs to draw attention to policies targeted for additional awareness throughout TSA. BOLOs are published throughout the year and written as changes occur at offices and airports nationwide. BOLOs are also written in response to actual SSI incidents at TSA HQ and field offices and from ideas and observations submitted by SSI Coordinators. BOLOs are crafted so that they will not contain SSI to allow their posting without concern that they can be viewed by the public.

The SSI Program office recommends all SSI Coordinators post BOLOs in common areas (e.g., break rooms, work spaces for screeners and stakeholders at airports) and include BOLOs in local newsletters so they are seen by as many personnel, stakeholders, and other covered persons as possible. These practices ensure covered persons are aware of SSI policy requirements. ***Note:*** *Many of these SSI Policy requirements serve as best practices for stakeholders.* Current and past BOLOs can be accessed by SSI Coordinators in the SSI Coordinators' Corner of the SSI Program office iShare page.

9.3 Bi-Monthly SSI Teleconferences

The SSI Program office schedules conference calls with SSI Coordinators and Area Coordinators every two months to discuss SSI updates and issues. Conference calls are also an opportunity for SSI Coordinators to submit ideas and recommendations for future SSI policies. For SSI Coordinators who cannot participate in the scheduled conference call, the SSI Program office makes the conference call available in a recorded form for one year following the call. SSI Coordinators can access these recordings by visiting the SSI Coordinators' Corner of the SSI Program office iShare page.

9.4 SSI Awareness Week

SSI Awareness Week, held annually during the first week of November, is intended to remind personnel of the importance of SSI and their responsibility to properly recognize, mark, protect, disclose, and destroy SSI. The SSI Program office attempts to engage personnel with activities such as crossword puzzles, word searches, quiz questions, training exercises, and other creative ideas.

One annual SSI Awareness Week activity is the nomination for the SSI Guardian Award. This award is presented to personnel who have recognized the importance of protecting SSI within the previous year and gone the extra mile to protect SSI. Nominees for the SSI Guardian Award are submitted to the SSI Program office at SSI@tsa.dhs.gov. The various activities provided by the SSI Program office for SSI Awareness Week are also available to SSI Coordinators in the SSI Coordinators' Corner of the SSI Program office iShare page.

9.5 SSI iShare Page & Internet Page

The SSI Program office relies on the SSI iShare Page to provide critical information to SSI Coordinators and other personnel. Applicable documents pertaining to the SSI Program and other guidance in recognizing, protecting, and handling SSI are available at this site.

The SSI Program office also maintains a public site available on the TSA homepage at http://www.tsa.gov/stakeholders/sensitive-security-information-ssi. This site contains information related to stakeholder and non-DHS training and policies.

9.6 Self-Inspection Program

Annually, each SSI Coordinator is required to complete the SSI self-inspection checklist and report results to the SSI Program. SSI Coordinators are also encouraged to conduct additional self-inspections throughout the year. The self-inspection checklist includes TSA-wide SSI programmatic requirements.

10.0 SSI Incidents

SSI Incident identification, response, and resolution are critical to TSA's ability to mitigate potential damage that may occur as a result of loss, compromise, unauthorized disclosure or mishandling of SSI.

10.1 Identifying SSI Incidents & SSI Password Incidents

SSI incidents are either major or minor:

SSI Incident (Major)

The verified or suspected loss, breach, or unauthorized disclosure of SSI to non-covered persons. The unauthorized disclosure of SSI to covered persons who do not have a need to know the information also shall be reported as a major SSI Incident. ***Note:*** *Depending on the circumstances, the SSI Program office may reduce incident to minor. The standard to be used in evaluating an SSI Incident as major or minor is whether there is a "reasonable suspicion" as to the loss or compromise of SSI*

- **Lost SSI:** SSI which, after reasonable attempts were made to find the material, cannot be located.
- **Breach of SSI:** SSI was accessible to or has been accessed by a non-covered person (e.g., the public).
- **Unauthorized Disclosure of SSI:** SSI was accessible to or has been accessed by a covered person who does not have a need to know the information.

SSI Incident (Minor)

The non-compliance with the TSA SSI Policies & Procedures Handbook in the handling of a record containing SSI that does not rise to the level of a major incident.

SSI Password incidents occur when:

- Any password created to encrypt SSI was not created or handled in accordance with the SSI Policies & Procedures Handbook; or
- The Standard TSA Password was sent to persons outside of DHS.

10.2 SSI Incident Response & Resolution

SSI incident response and resolution is a TSA-wide effort requiring the support and participation of many program offices. The SSI incident response and resolution process is composed of discovery and initial notification, immediate evaluation and follow-up notification, early mitigation, incident closure, long-term risk mitigation, and incident investigation (see Appendix 4: *SSI Incident Response Flow Chart*).

10.2.1 Discovery & Initial Notification

All personnel are responsible for identifying and reporting SSI incidents to their immediate supervisor and also to their designated SSI Coordinator. Personnel must also report routine mismarking of SSI to their SSI Coordinators. The SSI Coordinator is responsible for reporting major SSI incidents to the SSI Program office using the SSI incident reporting instructions (see Appendix 5: *SSI Incident Reporting Instructions*) as soon as possible, but no later than 8 hours after discovery. If, during the initial incident assessment, the SSI Coordinator determines the SSI Incident may be major, the SSI Coordinator must also notify the TSOC. ***Note:*** *OSO Field SSI Coordinators must report major SSI incidents to the TSOC through their Coordination Center.*

10.2.2 Immediate Evaluation & Follow-Up Notification

Once the SSI Program office receives the SSI incident report, SSI Program office personnel review the information and verify the SSI Coordinator's assessment as to whether the subject record is SSI. After processing the initial incident report, the SSI Program office will forward information on major incidents to the program owner of the information, Office of Chief Counsel (OCC), and other TSA headquarters offices, as appropriate:

- **Office of Inspection and the Chief Security Officer:** When a *TSA employee or contractor* is responsible for an SSI Incident
- **OSO Compliance Program:** When a *TSA stakeholder* is responsible for an SSI Incident
- **OIT CSIRT:** When an SSI Incident is *electronic* in nature
- **Office of Security Policy and Industry Engagement:** When subject SSI pertains to stakeholder assets
- **Strategic Communications and Public Affairs:** When an incident may generate media interest
- **Other Programs:** In addition to the program office that owns the subject SSI, the SSI Program office will notify other program offices whose functions or interests may be affected by the incident; when a *TSA contractor* is responsible for an SSI Incident, the affected program office's COTR may take appropriate action

If the SSI Program office, in consultation with the relevant program office, determines the records *do not contain SSI*, the SSI Program office relays this finding to the reporting SSI Coordinator and the incident is closed.

If the SSI Program office determines the records do contain SSI and the SSI Incident is major, the SSI Program office may recommend a team composed of members of affected program offices perform a damage assessment and affiliated risk mitigation (*see also* subsection 10.2.5 *Long-Term Risk Mitigation*).

10.2.3 Early Mitigation

The program office responsible for the incident and their SSI Coordinator must take reasonable steps to mitigate the effects of the SSI Incident. In incidents where no program office is clearly responsible, the SSI Program office coordinates early mitigation efforts.

Major SSI Incidents

- **Lost SSI:** Reasonable attempts to recover the materials (e.g., back-track through last known location, survey of other personnel with access to the area, review of CCTV footage covering the suspected location of the loss, etc.) must be undertaken. ***Note:*** *The major factor on whether lost SSI is a major or minor incident is the "reasonable suspicion" that the SSI was accessed by non-covered persons.*
- **Breach of SSI:** Reasonable attempts must be made to retrieve the content or limit further access by additional non-covered persons, unless such actions would draw more attention to the loss (consult with the SSI Program office, as necessary, to make this determination). Where appropriate, consider the use of NDAs for non-covered parties inadvertently receiving SSI to reduce the likelihood of further SSI incidents and breaches.
- **Unauthorized Disclosure of SSI:** Further access to the SSI must be restricted. Certain cases of unauthorized disclosure may not rise to the level of a major incident. Consult with the SSI Program office at SSI@tsa.dhs.gov to determine whether the improper disclosure is a major SSI incident.

Minor SSI Incidents

- **Mishandling of SSI:** Appropriately lock up or destroy SSI (*see also* subsection 5.0 *Safeguarding SSI*). Training and evaluation of safeguarding measures are appropriate to prevent further mishandling of SSI.

Note: *CSIRT assists in limiting access to the SSI on TSA iShare and network folders and may also assist in having SSI content removed from Internet pages when proper approvals are provided.*

10.2.4 Incident Closure

The SSI Program office considers SSI Incidents closed when the following have been met:

Major SSI Incidents

- **Lost SSI:** When all reasonable remedial and mitigating measures have been exhausted, though the SSI may remain beyond TSA's control.
- **Breach of SSI:** When all reasonable remedial and mitigating measures have been exhausted, though the SSI may remain beyond TSA's control.
- **Unauthorized Disclosure of SSI:** When only covered persons with a need to know the information may access it and, as practical, when all persons inappropriately receiving the information are notified not to further disseminate the SSI.

Minor SSI Incidents

- **Mishandling of SSI:** Closed by the SSI Coordinator upon receiving assurance from the appropriate office that procedures are in place to prevent recurrence.

Non-SSI Incident

- Incidents initially reported as SSI incidents are closed if the SSI Program office determines the information is not SSI, or for any other reason the SSI Program office determines the reported event does not constitute an SSI incident.

10.2.5 Long-Term Risk Mitigation

In some major incidents, it is appropriate for the program office that owns the SSI to lead an effort to perform a damage assessment, associated risk assessment, and complete a risk mitigation plan. If changes are made to processes or procedures in order to mitigate the effects of the incident or to prevent future incidents, the SSI Program office must be informed of the changes. If the affected program office creates an evaluation of the effect of the breach on its operations, the SSI Program office must be provided with the same. Feedback to the SSI Program office is key to ensuring these changes are incorporated into future SSI assessments and reviews.

The information owner is responsible for long-term risk mitigation. The SSI Program office may assist affected program offices, such as providing additional education and awareness regarding the proper handling and protection of SSI to prevent similar incidents from occurring. The information owner must also provide risk mitigation plans to the office's Information Protection Oversight Board (IPOB) representative for IPOB[26] review.

10.2.6 Incident Investigation

In some instances the Office of Inspection may open an investigation into the incident. In all investigations pertaining to SSI, the SSI Program office provides support to the office conducting the investigation, as appropriate, by providing a finding that SSI was or was not compromised in the incident. The SSI Program office may also supply the investigating authority with the data and information collected as part of the evaluation phase of the incident.

The investigating authority, if appointed, is responsible for final communication and reporting on SSI Incidents. SSI Incidents not warranting further investigation need not have detailed investigative closeout reports.

[26] The IPOB, established in June 2008 by the Deputy Administrator, was initially charged with implementing recommendations made by the Information Protection Commission. It continues today to serve as the internal, cross-agency forum for information protection policies and practices across TSA. It is comprised of senior-level representatives from each of TSA's Offices who are responsible for bringing their Offices' operational perspectives and requirements to Board deliberations. Board members represent and have the authority to speak for their Assistant Administrators and to drive information protection-related changes in their respective offices.

10.3 SSI Password Incident Response & Resolution

Personnel must immediately report password incidents to the SSI Program office at SSI@tsa.dhs.gov through the designated SSI Coordinator. The SSI Program office evaluates whether the password incident requires the issuance of a new Standard TSA Password. If a password incident *does* require the creation of a new Standard TSA password, the SSI Program office develops and distributes it to SSI Coordinators and other selected personnel via email.

The SSI Program office, in coordination with the SSI Coordinator, advises on other appropriate mitigation strategies for each unique password incident.

10.4 Penalties for Mishandling or Unauthorized Disclosure of SSI

Any TSA employee who violates TSA SSI policies and procedures may be subject to administrative and/or disciplinary action in accordance with TSA MD 1100.75-3, *Addressing Unacceptable Performance and Conduct*. TSA contractors who violate TSA SSI policies and procedures may be subject to administrative and/or disciplinary action as levied by the Contracting Officer.

Additionally, pursuant to 49 C.F.R. § 1520.17 and 49 U.S.C. § 46301(a)(4), civil penalties[27] for unauthorized SSI disclosure may include the following:

a. Aircraft Operators: Up to $27,500 per violation
b. Airport Operators: Up to $11,000 per violation
c. Individuals: Up to $11,000 per violation
d. Small Business: Up to $11,000 per violation
e. Rail Carriers, Receivers, and Shippers, and Passenger Transportation Agencies (Surface): Up to $10,000 per violation

If there are multiple violations, the maximum civil penalty per case is:

a. $50,000 for individuals and small business concerns
b. $400,000 for all other violators

[27] Numbers have been adjusted for inflation effective August 20, 2009.

11.0 Determining SSI Systems

In accordance with the *TSA Information Assurance Handbook*, all ISSOs are required to complete an SSI Threshold Analysis (SSITA) for their systems as part of the required documentation for their Security Authorization Package. The SSITA is required for the system owner to determine whether the systems process SSI and generally how that SSI is protected within these systems. An SSITA template is available at Appendix 6.

12.0 Protection Requirements for SSI Systems & Other Secure Sites

SSI may be shared with covered persons with a need to know through SSI Systems, including restricted networks (e.g., WebBoards), and other secure sites approved by TSA through the Security Authorization process as long as there are protections in place to ensure only covered persons with a need to know can access the information.

During the Security Authorization process, each ISSO is required to complete an SSITA as part of the system documentation (*see also* Section 11.0 *Determining SSI Systems*) and submit it to SSI@tsa.dhs.gov. Upon review of the SSITA, the SSI Program office may determine that additional documentation in the form of an SSI Impact Assessment (SSIIA) will be required for an SSI system and other secure sites. While completing an SSIIA for the systems, ISSOs should consider what SSI will be posted, how it will be posted, and any applicable restrictions to its access. ISSOs should also consider plans for training or verifying the training of SSI recipients, how the content will be reviewed periodically for usefulness, and how they will conduct audits of users to determine if they still have a need to know.

Per the Federal Information Processing Standard (FIPS) 199 and NIST 800-53, additional security controls may be required in addition to the minimum protection requirements. After reviewing a completed SSIIA, the SSI Program office, in coordination with OIT, determines whether any additional protection requirements are appropriate for the system.

Users of SSI Systems and other secure sites must be familiar with the terms of use for each particular system where they post SSI. These terms of use are frequently created in consultation with the SSI Program office. If a user is concerned with how the information is being handled on any particular site, contact the site administrator or the SSI Program office directly at SSI@tsa.dhs.gov. An SSIIA template is available at Appendix 7.

13.0 SSI Policy Exceptions

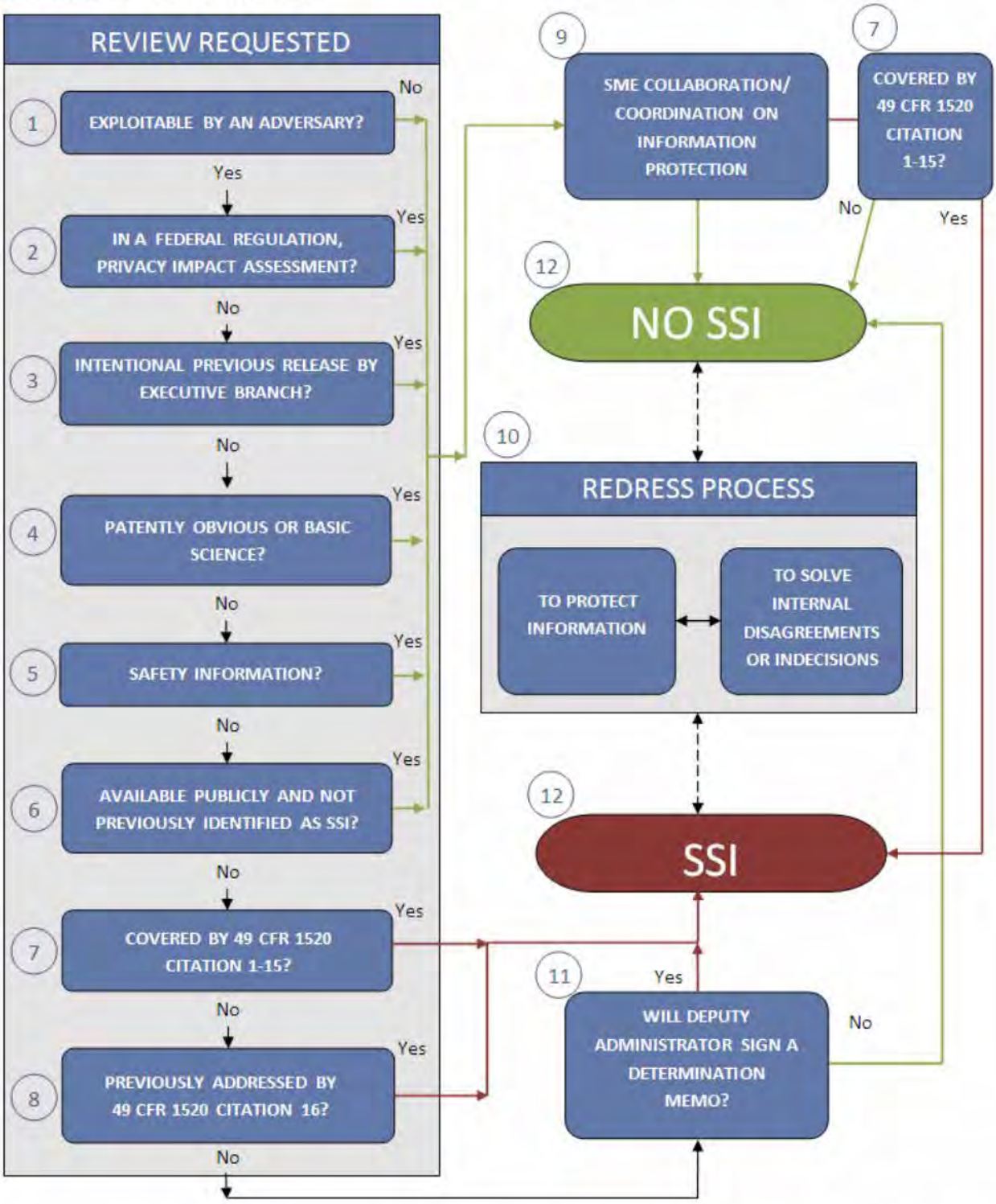
This Handbook is designed to meet the needs of personnel during the course of routine business. If an office or program must address a unique challenge with SSI, use the SSIIA template (at Appendix 7) to document this challenge, and submit the SSIIA to the SSI Program office at SSI@tsa.dhs.gov.

During periods of national emergency or exigent circumstances, the TSA Administrator or SSI Program Chief may determine that certain requirements of this Handbook should be temporarily suspended.[28] Even during national emergency or exigent circumstances, however, all covered persons are still required to take reasonable measures to protect SSI.

[28] Even if SSI Program office policies or procedures are temporarily suspended, other TSA program offices (e.g., Office of Information Technology's IAD) may have policies that still need to be followed.

Appendix 1: SSI Program Initial Decision Flow Chart

This product is designed to explain how the SSI Program office conducts its evaluations of information to determine if information warrants protection as SSI and whether that information protection is consistent with the SSI Regulation.



Flow Chart Notes

1. Exploitable by an Adversary?

Can the information be used to:

- Bring prohibited items into sterile areas?
- Defeat vetting processes?
- Avoid attention of Law Enforcement Officers/Intelligence?
- Target or avoid one screening method over another?

2. In a Federal Regulation or Privacy Impact Assessment?

- Is the information being reviewed publicly available in the Code of Federal Regulations?
- Is the information contained in a Privacy Impact Statement as required by the Privacy Act?

3. Intentional Previous Release by Executive Branch?

- Has an executive agency voluntarily released the information for public consumption?
- TSA/DHS press releases; information available on www.tsa.gov?
- Testimony in open session of Congress or unprotected court filings?
- Previous determinations by Administrator or SSI Program Chief?

4. Patently Obvious or Basic Science?

Would an average person, with some knowledge of the topic, be able to reasonably answer the question with confidence?

- Ex. "Do Federal Flight Deck Officers (FFDOs) carry their firearms in ordinary, non-descript bags?"
- Note: "Obvious" is admittedly subjective.

5. Safety Information?

- Does the information need to be widely known to ensure safe and efficient operation?
- Do first responders need to openly share this information for their own safety and the safety of others?

6. Available Publicly and Not Previously Identified as SSI?

Is the information available:

- Using a standard web search engine?
- On a Federal public web site?
- Note: Just because SSI information is on a known public site (except our own) does not mean we will not continue to protect the information.

7. Covered by SSI Regulation 49 C.F.R. § 1520.5(b)(1)-(15)?

- Do one of the 15 applicable categories of 49 C.F.R. § 1520.5(b)(1)-(15) apply?
- Is it contained in an SSI Identification Guide?
- Could a (16) determination be executed and legally sufficient to protect this information?

8. Covered by 49 C.F.R. § 1520.5(b)(16)?

Previous (16) determinations include:

- Aggregate Incident Data
- Railroad Automated Equipment Identification reader locations
- Names and identifying information on Office of Inspection Covert Testers

9. SME Collaboration/Coordination on Information Protection

SME COLLABORATION

- Engage program area SMEs to further explain rationale for release or protection.
- Include other TSA offices which may have equities.

SME COORDINATION

- Based on past practice, written guidance or confirmed specific concurrence, do the SMEs concur that the information should be protected?

10. Redress Process

Appeals of previous SSI findings undergo a re-review with emphasis on additional SME input and cost/burden input from appellant.

11. Will Deputy Administrator Sign a Determination Memo?

The recommended (16) determination is socialized then processed through ExecSec for concurrence and Deputy Administrator signature.

12. SSI? Yes/No

- Will the information be protected as SSI?
- Do we have concurrence within the SSI Program office?
- Does the SSI Program office require additional support from an AA or the Administrator to protect or release this information?

Appendix 2: SSI Coordinator Designation Instructions

Notification of appointments to SSI Coordinator positions should be sent by the appointing official (i.e., FSD, FAM SAC, or AA) to the SSI Program office via email to SSI@tsa.dhs.gov with a courtesy copy to the appointee. The notification should include the appointee's:

(1) Name

(2) Official position/title

(3) Identification as either the Primary or Alternate Coordinator

(4) Phone number

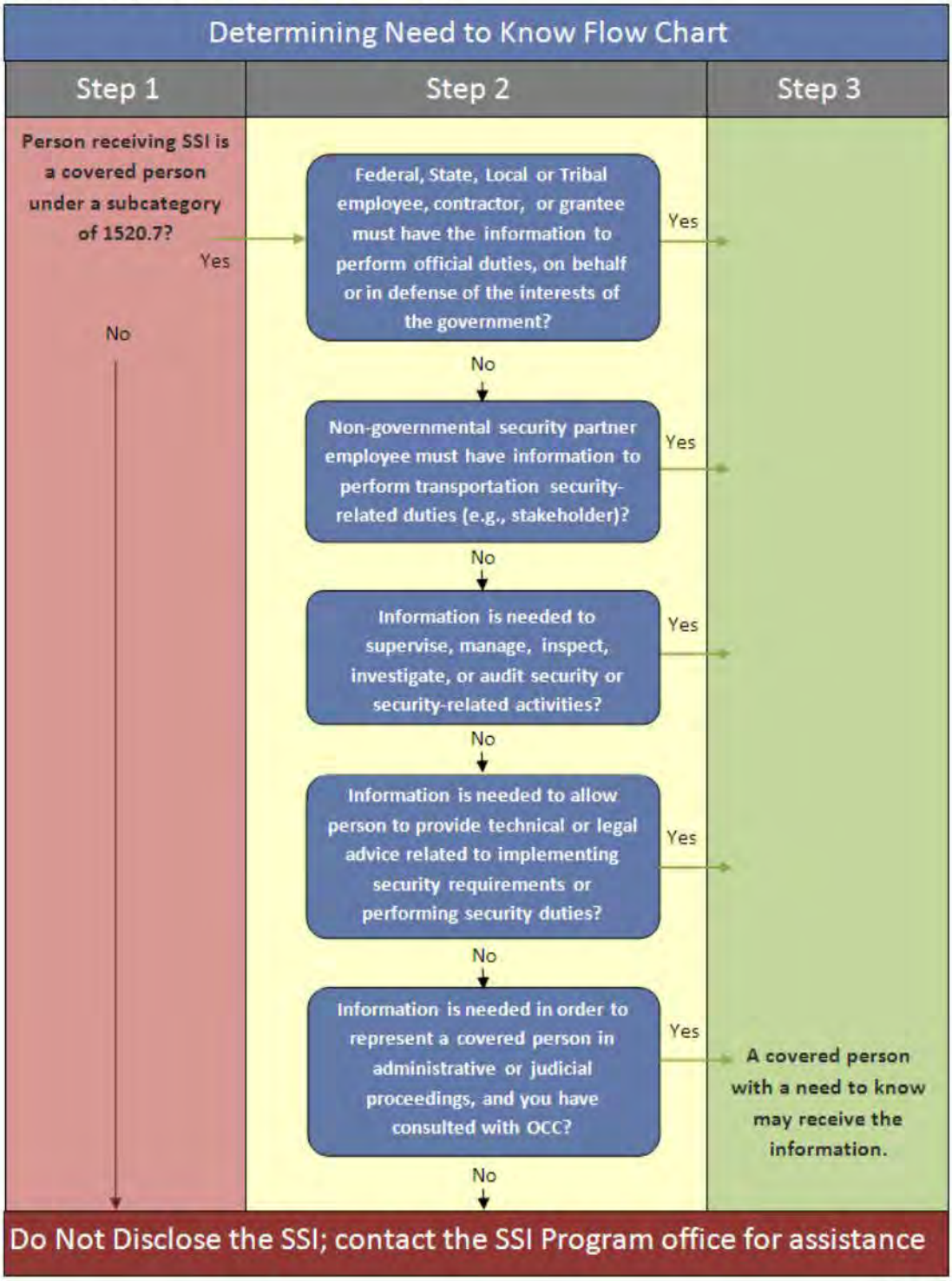
(5) Email address

(6) TSA headquarters or field office, city, state & airport code (if applicable)

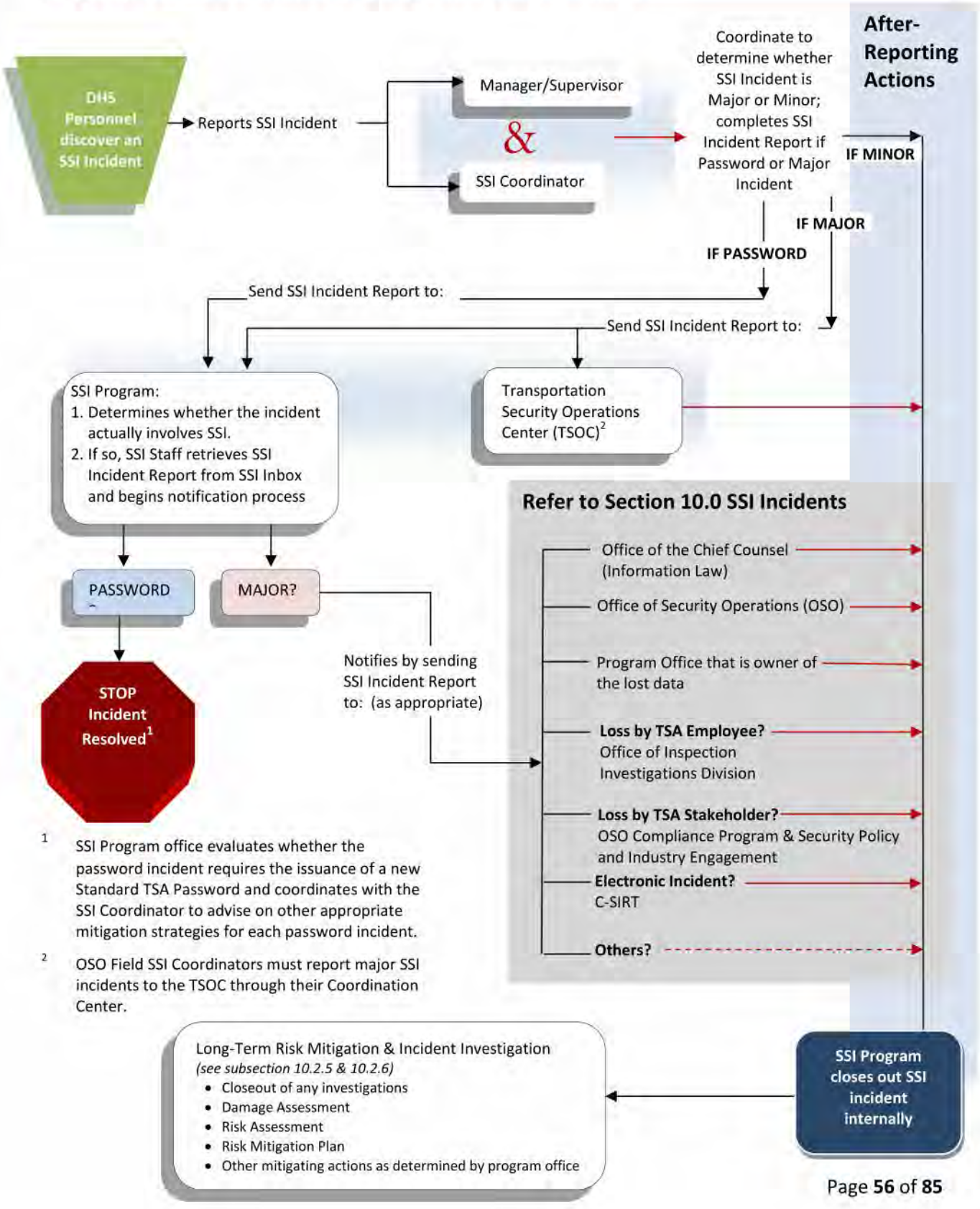
A sample SSI Appointment Letter is available on the SSI iShare homepage which includes a full listing of SSI Coordinator responsibilities. The SSI Program recommends filing a copy of the appointment letter in the SSI Coordinator's personnel file.

Appendix 3: Determining Need to Know Flow Chart

This product is intended for general use outside of the SSI Program office. It was designed to assist personnel in determining whether an individual or group has a need to know SSI and if that information sharing is consistent the SSI Regulation 49 C.F.R. §§ 1520.7 and 1520.11. If further guidance is needed, contact the SSI Program office at SSI@tsa.dhs.gov.



Appendix 4: SSI Incident Response Flow Chart

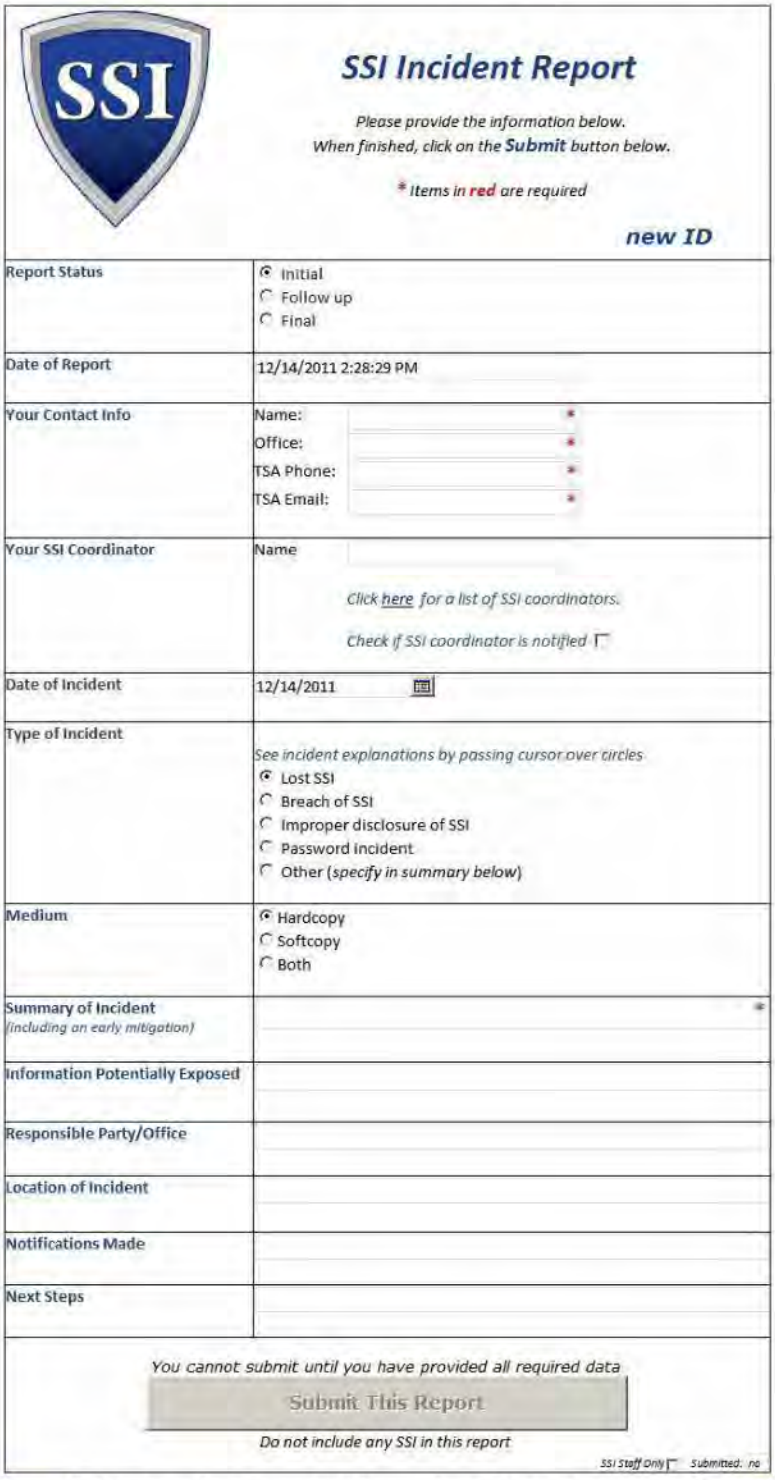


1 SSI Program office evaluates whether the password incident requires the issuance of a new Standard TSA Password and coordinates with the SSI Coordinator to advise on other appropriate mitigation strategies for each password incident.

2 OSO Field SSI Coordinators must report major SSI incidents to the TSOC through their Coordination Center.

Appendix 5: SSI Incident Reporting Instructions

When reporting SSI Incidents to the SSI Program office, refer to subsection 10.0 *SSI Incidents* and Appendix 4: *SSI Incident Response Flow Chart* and ensure to include the following details:



SSI Incident Report

Please provide the information below.
When finished, click on the ***Submit*** *button below.*

* *Items in* ***red*** *are required*

new ID

Report Status	◉ Initial ○ Follow up ○ Final
Date of Report	12/14/2011 2:28:29 PM
Your Contact Info	Name: * Office: * TSA Phone: * TSA Email: *
Your SSI Coordinator	Name *Click here for a list of SSI coordinators.* *Check if SSI coordinator is notified* ☐
Date of Incident	12/14/2011
Type of Incident	*See incident explanations by passing cursor over circles* ◉ Lost SSI ○ Breach of SSI ○ Improper disclosure of SSI ○ Password incident ○ Other (*specify in summary below*)
Medium	◉ Hardcopy ○ Softcopy ○ Both
Summary of Incident *(including an early mitigation)*	*
Information Potentially Exposed	
Responsible Party/Office	
Location of Incident	
Notifications Made	
Next Steps	

You cannot submit until you have provided all required data

Submit This Report

Do not include any SSI in this report

SSI Staff Only ☐ *Submitted: no*

An InfoPath version of this template is available on the TSA SSI Program office iShare homepage.

Appendix 6: SSI Threshold Analysis

Transportation Security Administration

Transportation Security Administration
Office of Law Enforcement/Federal Air Marshal Service
Office of Security Services and Assessments

SSI Threshold Analysis

Appendix 6 to SSI Policies & Procedures Handbook

Version 1

SSI Program
Current as of 23 April 2012

Sensitive Security Information (SSI)
Threshold Analysis

The purpose of this SSI Threshold Analysis is to determine where SSI (as defined in 49 C.F.R. Part 1520) resides in electronic form within TSA IT systems and generally how that SSI is protected within these systems. Email the completed document to the SSI Program office for review at SSI@tsa.dhs.gov.

Upon receipt, the SSI Program office may contact you for further information and/or documentation. The TSA SSI Program office will review this SSI Threshold Analysis and advise you of the final SSI determination and whether it is necessary to fill out an SSI Impact Assessment.

This document should also be used by emerging and standing security programs and initiatives to determine whether it may be appropriate to develop an SSI Identification Guide, in coordination with the SSI Program office. Additionally, this document should be included as part of the TSA certification and accreditation document suite.

SSITA must be completed (1) during each review of Authorization to Operate (ATO); (2) during any significant modification or update to the system impacting information available on the system; or (3) every three years, whichever event occurs first.

A copy of this template is available on the TSA SSI Program office iShare homepage.

Definitions of Terms Used

General Support System: A General Support System (GSS) is an interconnected set of information resources under the same direct management control which shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. A GSS provides a supporting infrastructure and/or services to allow other applications to function. All GSS must have one or more Information Systems Security Officers (ISSO) assigned. Examples of a GSS are:

- A local area network (LAN) or wide-area networks, including terminals supporting the network;
- A communications network, including switches, routers, and hardware components;
- A departmental data processing center including its operating system, utilities, and personnel; and
- A shared information processing service organization.

Information Owner: The TSA individual or office with responsibility for and the authority to determine the allowable uses of the data sought as part of a routine or ad hoc Computer Readable Extract (CRE). With some systems, the Information Owner may also be the Business Owner or System Owner. The Information Owner is responsible for ensuring that all media containing SSI is appropriately marked and for designating, in writing, the use of and restrictions to access to SSI.

Information System: A discrete set of information resources, either in stand-alone or networked configuration, which is organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

Information System Security Officer (ISSO): The TSA individual responsible for information security on an assigned set of systems or locations. The TSA ISSOs report directly to the TSA CISO for matters related to information security.

Major Application: A Major Application (MA) is an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. All Federal applications require some level of protection; however, certain applications require special management oversight and additional security due to the sensitivity of information they contain. The system exposure, location, and sensitivity analysis help determine if the special attention is required. A Major Application directly supports a Component's mission(s) or helps sustain day-to-day operations. Examples may include payroll systems, inventory systems, transaction processing systems, and record management systems. All MA must have one or more Information Systems Security Officers (ISSO) assigned.

Minor Application: When an application does not meet the criteria for a Major Application but still requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application, it is defined as a Minor Application. A Minor Application is either a Component application of a Major Application or resides on a General Support System and it is provided security via the umbrella under which it operates [OMB A-130]. The main difference between Major Applications and Minor Applications is mission criticality. A non-mission critical system is most likely a Minor Application or subsystem. Minor Applications are typically included as part of a GSS.

System Owner: The TSA Government Official responsible for using information technology to help achieve the mission needs within their area of responsibility; also responsible for the successful operation of the information systems within their division and are ultimately accountable for their security.

Sensitive Security Information (SSI)
Threshold Analysis

PART A

Does Your Information System/Program Store, Transmit or Process Any Category of Information Listed Below?

(Check all that apply)

1. ☐ **Security programs or contingency plans**. Any security program or security contingency plan issued, established, required, received, or approved by the Department of Transportation (DOT) or the Department of Homeland Security (DHS), including any comments, instructions, or implementing guidance pertaining thereto.

   Examples: Corporate Security Plans, Aircraft Operator Standard Security Programs, Airport Security Programs, other security programs for certain modes of transportation.

2. ☐ **Security Directives/Emergency Amendments**. Any Security Directive/Emergency Amendment or order issued by TSA under 49 C.F.R. 1542.303, 1544.305, 1548.19 or other authority, including any comments, instructions, and implementing guidance pertaining thereto.

   Examples: TSA Office of Security Operations Security Directives (SDs), Airport and Indirect Air Carrier (IAC) SDs and Emergency Amendments.

3. ☐ **Information Circulars**. Any notice issued by DHS/DOT components regarding a threat to aviation or maritime transportation.

   Examples: TSA-issued Information Circular-type notices that contain SSI.

4. ☐ **Performance specifications**. Any performance specification and any description of a test object or test procedure, for –

   (i) Any device used by the Federal Government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any person, and any weapon, explosive, incendiary, or destructive device, item, or substance; and

   Examples: Performance specifications in pre-award acquisition actions.

   (ii) Any communications equipment used by the Federal Government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

   Examples: Performance and test data; descriptions of test objects used for covert testing.

5. ☐ **Vulnerability assessments**. Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

   Examples: Pre-planned security audits, tests, and vulnerability assessments (not incident-related).

6. ☐ **Security inspection or investigative information**. Details of any security inspection or investigation of an alleged violation of aviation, maritime, or rail transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal agent or other Federal employee who conducted the inspection or audit, and summaries of this inspection or investigative information within 12 months of the date of the release of the inspection or investigative information.

   Examples: Unplanned (incident- or violation-related) inspection or investigative information that reveals a vulnerability.

7. ☐ **Threat information**. Any information held by the Federal Government concerning threats against transportation or transportation systems, sources or methods used to gather or develop threat information, including threats against cyber infrastructure.

   Examples: Threat information in an incident report; details of bomb threat.

8. ☐ **Security measures**. Specific details of aviation, maritime, or rail transportation security measures, both operational and technical, including security measures or protocols recommended by the Federal Government; information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals (to the extent it is not classified national security information); information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator; and any armed security officer procedures issued by TSA under 49 C.F.R. Part 1562.

   Examples: Non-screening security measures; Federal Air Marshal/Federal Flight Deck Officer (FAM/FFDO) deployments and operations and FAM numbers.

9. ☐ **Security screening information**. The following information regarding security screening under aviation or maritime transportation security requirements of Federal law:

   (i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal Government or other authorized person.

   (ii) Information and sources of information used by a passenger or property screening program or system including an automated screening system.

   (iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI.

   (iv) Any security screener test and scores of such tests.

   (v) Performance or testing data from security equipment or screening systems.

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images or threat image projection systems.

Examples: Checkpoint Screening Standard Operating Procedures (SOP); Management Screening SOP; Checked Baggage SOP; security screening procedures; screener test scores; electronic images from screening monitors.

10. ☐ **Security training materials**. Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal Government or another person to carry out any aviation, maritime, or rail transportation security measures required or recommended by DHS or DOT.

Examples: Behavior Detection Officer training manuals; training materials related to security.

11. ☐ **Identifying information of certain transportation security personnel**.

(i) Lists of names or other identifying information that identify persons as:

(A) Having unescorted access to a secure area of an airport, a rail secure area, or a secure or restricted area of a maritime facility, port area, or vessel.

(B) Holding a position as a security screener employed by or under contract with the Federal Government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport.

(C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection.

(D) Holding a position as a Federal Air Marshal; or

(ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.

Examples: Lists of Aviation Security Inspectors (ASIs), lists of all Transportation Security Officers (TSOs) at an airport; lists of FAM names; individual FFDO names and lists of FFDO names; consult SSI Program office for other identifying information.

12. ☐ **Critical aviation, maritime, or rail infrastructure asset information**. Any list identifying systems or assets, whether physical or virtual, so vital to the aviation, maritime, or rail transportation system (including rail hazardous materials shippers and rail hazardous materials receivers) that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is prepared by DHS or DOT or prepared by a State or local government agency and submitted by the agency to DHS or DOT.

Examples: Used very infrequently; consult SSI Program office.

13. ☐ **Systems security information**. Any information involving the security of operational or administrative data systems operated by the Federal Government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

Examples: Security information on IT systems that are critical; consult SSI Program office.

14. ☐ **Confidential business information**.

    (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising there from, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures.

    (ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities.

    (iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

    Examples: Rarely used; consult SSI Program office.

15. ☐ **Research and development**. Information obtained or developed in the conduct of research related to aviation, maritime, or rail transportation security activities, where such research is approved, accepted, funded, recommended or directed by DHS or DOT, including research results.

    Examples: Next generation of screening equipment test results; consult SSI Program office.

16. ☐ **Other information**. Any information not otherwise described in 49 C.F.R.§1520.5(b) that TSA determines is SSI under 49 U.S.C. § 114(r) or that the Secretary of DOT determines is SSI under 49 U.S.C. § 40119. Upon the request of another Federal agency, TSA or the Secretary of DOT may designate as SSI information not otherwise described in this section.

    Examples: Aggregate Incident Data; Railroad Automated Equipment Identification reader locations; Names and identifying information on OOI Covert Testers; consult SSI Program office.

Sensitive Security Information (SSI)
Threshold Analysis

PART B

Summary of the System

DATE **submitted for review:**
NAME **of** System: <Please enter the name.>
Name of Information Owner: <Please enter the name.>
Email for Information Owner: <Please enter the email address.>
Phone number for Information Owner: <Please enter the phone number.>

Name of System Owner: <Please enter the name.>
Email for System Owner: <Please enter the email address.>
Phone number for System Owner: <Please enter the phone number.>

Name of ISSO: <Please enter the name.>
Email for ISSO: <Please enter the email address.>
Phone number for ISSO: <Please enter the phone number.>

TYPE **of System:**

- ☐ General Support System
- ☐ Major Application
- ☐ Minor Application
- ☐ Non-TSA System

Status of System:

- ☐ This is a new development effort undergoing **initial Security Authorization**.
- ☐ This is an operational system going through **reauthorization**.
- ☐ This is a non-TSA system which does not require **Security Authorization**.

(System Owner, Information Owner and ISSO must sign endorsements in Part E.)

Sensitive Security Information (SSI)
Threshold Analysis

PART C

Description of the System and Its Purpose

- List the system name and the name of the Department component(s) that own(s) the system.
- Describe the purpose of the system, the authorizing legislation, and how it relates to the Agency's mission.
- Describe how the system collects and uses SSI, including a typical transaction that gives the life cycle from collection/creation to destruction of SSI.
- Describe any information sharing conducted by the system.
- Describe the major potential risks of unauthorized disclosure or mishandling within the program and steps the program has taken to protect SSI and mitigate the risks of unauthorized disclosure of SSI.
- **Note:** Do not list every risk of unauthorized disclosure in the preceding analysis section. Rather, provide a holistic view of the risks to SSI. Describe any routine information sharing conducted by the system both within TSA and other DHS components and with external sharing partners. Describe how such external sharing is compatible with the original collection or creation of SSI.
- Identify the technology used and provide a brief description of how it maintains SSI for the system, including a confirmation that the technology is approved or is in the process of being approved by the TSA Office of Information Technology for the maintenance of SSI via an Authorization to Operate (ATO).

Sensitive Security Information (SSI)
Threshold Analysis

PART D

SSI Use & Impact Assessment Determination

(To Be Completed by the TSA SSI Program office)

Date reviewed by the SSI Program office:

Name of the SSI Program Office Reviewer: <Please enter name of reviewer.>

SSI Use Determination

☐ This system DOES NOT collect, process, maintain, use, share, disseminate, or dispose of SSI.

☐ This system DOES collect, process, maintain, use, share, disseminate, or dispose of SSI.

SSI Impact Assessment Requirement Determination

☐ This system WILL require the completion of an SSI Impact Assessment to accompany this SSI Threshold Analysis as part of the Security Authorization Package.

☐ This system WILL require the completion of an SSI Impact Assessment to document alternate acceptable protection in lieu of standard SSI policies and procedures (For use only by smaller systems or other secure sites not requiring Security Authorization.)

☐ This system WILL NOT require the completion of an SSI Impact Assessment at this time.

Sensitive Security Information (SSI)
Threshold Analysis

PART E
Endorsements

Note: Endorsement by the SSI Program office on this SSI Threshold Analysis does not remove the applicant's requirement to complete other documentation which may be required by other program offices. ISSO and CISO signatures are only required when the SSITA will be used as part of a Security Authorization package.

_____ _____

ISSO **Date**

_____ _____

System or Program Owner (as appropriate) **Date**

_____ _____

Information Owner (Assistant Administrator)[29] **Date**

_____ _____

TSA SSI Program Office Reviewer **Date**

_____ _____

CISO **Date**

[29] For multiple types of information, add more Information Owner lines.

Appendix 7: SSI Impact Assessment

Transportation Security Administration

Transportation Security Administration
Office of Law Enforcement/Federal Air Marshal Service
Office of Security Services and Assessments

SSI Impact Assessment

Appendix 7 to SSI Policies & Procedures Handbook

Version 1

SSI Program
Current as of 23 April 2012

Sensitive Security Information (SSI)
Impact Assessment

The purpose of this SSIIA is to determine how SSI (as defined in 49 C.F.R. Part 1520) is being protected within TSA IT systems; to verify compliance with SSI policies and procedures; and, if necessary, to propose alternate acceptable protection in lieu of standard SSI policies and procedures.

The TSA SSI Program office will review this SSIIA and advise if additional protections will be required for the system seeking Security Authorization through the Office of Information Technology (OIT). This SSIIA may also be used by other non-TSA systems or other secure sites not requiring Security Authorization to document alternate acceptable protection in lieu of standard SSI policies and procedures.

Use the attached template to complete the SSIIA as required by TSA MD 2810.1, *SSI Program*, TSA SSI Policies & Procedures Handbook, or SSI Threshold Analysis (SSITA). Submit the completed SSIIA to the TSA SSI Program office at SSI@tsa.dhs.gov for review. Upon receipt, the SSI Program office may contact the sender for further information and/or documentation.

SSIIA must be completed (1) during each review of Authorization to Operate (ATO); (2) during any significant modification or update to the system impacting users or information available on the system; or (3) every three years, whichever event occurs first.

A copy of this template is available on the TSA SSI Program office iShare homepage.

SENSITIVE SECURITY INFORMATION IMPACT ASSESSMENT
for the

<<ADD NAME>>

<<ADD Publication Date>>

Contact Point
<<ADD Contact Person>>
<<ADD Contact Phone>>

Reviewing Official
Name
Chief, SSI Program
(571) 227-(b)(6)

Abstract

The abstract is a single paragraph that describes the program and the SSIIA. It will be published on the SSI iShare site. It should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- *First sentence should include the name of the component or program office and the system.*
- *Second sentence should be a brief description of the system and its function.*
- *Third sentence should explain the reason the system is being created and why the SSIIA is required. This sentence should embody an analysis of the role of SSI in the program.*

<<ADD Abstract here>>

Overview

The overview creates the foundation for, and provides an introduction to, the entire SSIIA. The overview provides the context and background necessary to understand the system's purpose and mission and the justification for operating a program that incorporates the collection, creation or use of SSI. Include the following:

- *List the system name and the name of the Department component(s) that owns the system.*
- *Describe the purpose of the system, the authorizing legislation, and how it relates to the Agency's mission.*
- *Describe how the system collects and uses SSI, including a typical transaction that gives the life cycle from collection/creation to destruction of SSI. If multiple transaction methodologies are used, include a description of each type.*
- *If applying for alternate acceptable protections in lieu of current SSI Policies & Procedures, list the SSI Program policies for which the applicant seeks a waiver.*
- *Describe any information sharing conducted by the system.*
- *Describe the major potential risks of unauthorized disclosure or mishandling within the program and how the program has taken steps to protect SSI and mitigate the risks of unauthorized disclosure of SSI. This description should include both technical and procedural processes in place.*[30]
- *Identify the technology used and provide a brief description of how it maintains SSI for the system, including assurance confirmation that the technology is approved (or is in the process of being approved) by the TSA Office of Information Technology for the*

[30] ***Note:*** *Do not list every risk of unauthorized disclosure in the preceding analysis section. Rather, provide a holistic view of the risks to SSI. Describe any routine information sharing conducted by the system both within TSA and other DHS components and with external sharing partners. Describe how such external sharing is compatible with the original collection or creation of SSI.*

maintenance of SSI via an Authorization to Operate (ATO). Include descriptions of any encryption mechanisms in place.

- *If this document is being used to apply for an exception to TSA SSI policies and procedures, list here any exceptions requested for policies or procedures.*

<<ADD Introduction Here>>

Section 1.0 - Authorities

1.1 Has the system's configuration control been approved for the management of SSI by the TSA Office of Information Technology?

Provide the date that the most recent ATO was granted or, if a new system, the date ATO is expected to be awarded. An operational system must comply with DHS Policy Directive 4300A, DHS Sensitive Systems Policy. If this SSIIA is being completed as part of a Security Authorization package, please state that here.

<<ADD Answer Here>>

Section 2.0 - Characterization and Uses of SSI

The following questions are intended to define the scope of the information created and/or collected, as well as reasons for its creation or collection.

2.1 Identify the SSI that the system collects, stores or disseminates. Describe how and why the system creates, collects and uses SSI.

Identify the categories of SSI, as defined in the SSI Regulation, 49 C.F.R.§1520.5(b)(1)–(16) that are created, collected, or used by the system and the utility of this information system.[31]

<<ADD Answer Here>>

[31] *Note: This could include Security Directives or Information Circulars, equipment or personnel performance specifications, vulnerability assessments, security inspection or investigative information, threat information, security measures, security screening information, security training materials, identifying information or designated transportation security personnel, critical aviation or maritime infrastructure asset information, systems security information, confidential business information, or research and development information. It could also include any information that otherwise falls into one of the 15 delineated categories of SSI in 49 C.F.R. § 1520.5(b)(1)–(15) or information that has been designated as SSI under the authority of 49 C.F.R. §1520.5(b)(16).*

If the system receives SSI from another office or system, describe the office or system from which the information originates, including any information that is returned and how the received SSI is then used and who has access to the SSI.

<< ADD Answer Here>>

Describe the mechanism used to share and distribute the SSI to other offices. Include a discussion of how transmission of the SSI is secure and complies with TSA requirements for safely transmitting and sharing SSI.

<<ADD Answer Here>>

2.2 What are the media formats of the SSI?

Include how the SSI is conveyed (e.g., multimedia formats, such as audio or video files). If the SSI is received electronically, describe the security controls in place to ensure that the confidentiality of the information is maintained to individuals with a need to know.

<<ADD Answer Here>>

2.3 Discuss how the correct determination of information as SSI or non-SSI is assured.

Explain how the information owner ensures records or documents are properly identified and labeled as SSI, and how the system reviews information that is received by the system from another source to determine whether it is properly marked.

Explain how the System Owner has consulted with their appointed SSI Coordinator. Explain efforts to provide SSI education and awareness to system staff.[32]

<<ADD Answer Here>>

[32] *Note: SSI Program office provides Advanced SSI Training to data managers or others responsible for monitoring site content. For more information, contact the SSI Program office at SSI@tsa.dhs.gov.*

Section 3.0 - Data maintenance and information sharing by the system

3.1 How is the SSI maintained by the system?

Discuss the risks associated with maintenance of the SSI created, collected or maintained by the system. What controls are enforced by the system to mitigate those risks, i.e., steps taken by the system to appropriately safeguard and protect the SSI from unauthorized disclosure.

Discuss any risks of the SSI being disclosed to non-covered persons or covered persons who do not have a need to know the information. Include a discussion of technological safeguards utilized by the system in the creation, collection, maintenance, dissemination, and destruction of SSI. Discuss the extent to which any electronic database or other system of records management used to maintain SSI incorporates SSI safeguard measures.

<<ADD Answer Here>>

3.2 Is SSI shared outside of TSA as part of normal system operations? If so, identify the organization(s) or person(s) with whom the SSI is shared, how the information is accessed by those entities, and how they use the SSI.

Discuss the external sharing of SSI (for example, TSA to CBP or TSA to an air carrier). Identify the name or names of the Federal agencies or others who will receive SSI through or on behalf of the system. Identify how the SSI is used by each external person or office with whom it is shared. Discuss how the external persons or office will be provided SSI education and awareness training.

For State, local, or tribal governments, or private sector organizations, list the general types rather than the specific names of these organizations.

<<ADD Answer Here>>

3.3 Does the system place limitations on distribution?

Describe any limitation that may be placed on external agencies or entities from further sharing the SSI provided by the system. In particular, describe how the system makes a determination as to which covered persons with a need to know will have access to the information. Describe any mechanisms or procedures put in place to ensure that SSI is not further disseminated beyond those individuals with whom the system has shared the SSI. Discuss the extent to which the Terms of Use of any electronic database or other system of records management used to maintain SSI places limitation on further distribution of the information. Describe protocols that have been designed to report an unauthorized disclosure of SSI.

<<ADD Answer Here>>

3.4 What are the Risks of Unauthorized Disclosure Related to Information Sharing?

Discuss the risks of unauthorized disclosure (e.g., an instance in which the SSI is accessed by covered persons who do not have a need to know or non-covered persons who are not authorized by the system) associated with the sharing of SSI outside of the Agency. Discuss how these risks are mitigated.

Discuss whether access controls have been implemented to ensure appropriate sharing outside of TSA. If remote access to a system is allowed to transmit SSI, describe any measures in place to secure the transmission (e.g., encryption of data in transit). If external storage is used to store SSI or if communication devices interact with the system, describe any measures in place to secure data (e.g., data at rest encryption, two-factor authentication).

Discuss how the sharing of information outside of TSA is compatible with the stated purpose of the original creation, collection, or use of SSI.

<<ADD Answer Here>>

3.5 Does the site or system maintain a Terms of Use Agreement or pre-use notification of required SSI protections and limitations on distribution?

Discuss how the Terms of Use Agreement or other pre-use notification is made available to the site or system user.

Discuss the frequency of user acknowledgement of the site or system Terms of Use Agreement.

<<ADD Answer Here>>

<<ADD Terms of Use Agreement Here>>

Section 4.0 Auditing and Accountability

The following questions are intended to describe technical, regulatory, and policy based safeguards and security measures.

4.1 How does the System Owner or Information Owner ensure that the SSI is used in accordance with the stated practices in this SSIIA?

Discuss how the system uses technical and policy safeguards required by 49 C.F.R. Part 1520 and the SSI Policies & Procedures Handbook issued by the TSA SSI Program office. Also describe any additional safeguards or controls used by the system to adhere to this SSIIA. Include an assurance that the system's program has an SSI Coordinator, certified by the TSA SSI Program office, who conducts an annual self-inspection of the system as required by TSA MD 2810.1, SSI Program. If the SSI Coordinator for the system has not yet been appointed, provide the anticipated date of the appointment. Likewise, if the SSI Coordinator for the system has not yet been certified, provide the anticipated date on which he or she will attend Advanced SSI Training & Certification.

<<ADD Answer Here>>

4.2 Describe how the System Owner or Information Owner ensures SSI training is provided to system employees and personnel and to users and recipients of SSI that is distributed by or on behalf of the system.

TSA provides SSI training for all employees and contractors through the Online Learning Center or as requested by independent programs. Each system may offer training specific to the system, which touches on SSI handling procedures, identification, and any unique system-specific concerns. Discuss how individuals who have access to SSI through the system are trained to appropriately recognize, safeguard, and destroy the information. TSA also provides handling guides for DHS or non-DHS employees, as appropriate.

Will the system require specialized SSI training provided by the TSA SSI Program office?

<<ADD Answer Here>>

4.3 How does the System Owner review and approve Interconnection Security Agreements (ISAs), Memorandums of Understanding (MOUs), new uses of SSI or new access to the system by offices within TSA and outside entities?

Describe the procedures utilized by the system to approve the sharing of SSI with covered persons who have an operational need to know the information.

<<ADD Answer Here>>

Section 5.0 Additional Protections Required

The following section must be filled out by the SSI Program office reviewer, in conjunction with the System Owner and OIT's Information Assurance Division.

5.1 Are there additional protections required above the minimum Federal Information Processing Standard (FIPS) 199 impact level of "Moderate" or higher for confidentiality and integrity in order for this system to be approved as an SSI system?

Based upon the sensitivity of the information and vulnerability to access as noted within this document, describe any additional protections which would mitigate against information compromise.

<<ADD Specific FIPS impact level high requirements here>>

Responsible Officials

<<ADD System Owner and SSI Coordinator for Program Office which owns the system>>

Transportation Security Administration

Endorsements[33]

Signatures below signify concurrence with proposed protections as annotated in this SSI Impact Assessment. Any failure by the System Owner to apply protections as annotated in this document nullifies below approvals.

ISSO **Date**

System or Program Owner (as appropriate) **Date**

Information Owner (Assistant Administrator)[34] **Date**

TSA SSI Program Office Reviewer **Date**

CISO **Date**

[33] **Note:** Endorsement by the SSI Program office on this SSI Impact Assessment does not remove the applicant's requirement to complete other documentation which may be required by other program offices. ISSO and CISO signatures are only required when the SSIIA will be used as part of a Security Authorization Package.

[34] For multiple types of information, add more Information Owner lines.

Appendix 8: Determining SSI Release to Foreign Governments

Step 1: DHS or DOT component drafts SSI document.
Step 2: DHS or DOT component shares SSI document with Intelligence Community (IC).
Step 3: Member of IC wants to disclose to foreign government.
Step 4: Member of IC submits request for disclosure of SSI to foreign government not otherwise covered under 49 C.F.R. Part 1520 to SSI@tsa.dhs.gov.
Step 5: SSI Program In-Box evaluates which component created the SSI.
Step 6: SSI Program routes SSI to representative of component owning the SSI.
Step 7: Component representative coordinates with information owner to determine if disclosure appropriate.
Step 8: DOT, USCG, or TSA representative crafts determination.
Step 9: DOT, USCG, or TSA signatory authority signs determination (for both approval and disapproval).
Step 10: Component representative returns the determination to SSI at SSI@tsa.dhs.gov for return to requestor.

Appendix 9: Instructions for New SSI Coordinators

Newly-appointed SSI Coordinators have a number of administrative and training requirements to register in the SSI Program system and become certified as an SSI Coordinator. *New SSI Coordinators working through this process should contact the SSI Program Office at SSI@tsa.dhs.gov with any questions regarding their new responsibilities or requirements.*

Getting Started

- Notify the SSI Program of new SSI Coordinator appointment through the SSI Coordinator InfoPath Form. The SSI Coordinator InfoPath form will be disseminated with Instructions for New SSI Coordinators, and should be filled out completely with contact information, Coordinator status, and other select data.
- Ensure an SSI Coordinator Appointment Letter is completed, signed, and placed in the new SSI Coordinator's personnel file since this is a collateral duty.
- Within one week of receipt of the contact information, the SSI Program will grant the new SSI Coordinator access to the SSI Coordinator's Corner, an iShare site that contains many resources for SSI Coordinators. In the meantime, information regarding SSI ID Guides, policy documents, and other guidance can be found on the SSI Program iShare site.
- Within one week of receipt of the contact information, the new SSI Coordinator will be added to the SSI Coordinator's Contact List. Inclusion on the SSI Coordinator's Contact list will allow new appointees to immediately start receiving communication from the SSI Program office on any SSI-related information such as BOLOs, SSI Bi-Monthly Teleconferences, Password Changes, etc.

Attending Advanced SSI Training and Certification Course

One of the first things the new SSI Coordinator needs to do is get enrolled in an upcoming Advanced SSI Training and Certification course. Every new SSI Coordinator is required to attend the Advanced Certification Training and pass the Certification Exam, provided by the SSI Program, within one year of appointment. The SSI Program recommends that new SSI Coordinators take this training as soon as possible to become familiar with identifying SSI and requirements for handling SSI to prepare them for their new collateral duties. The SSI Coordinator InfoPath Form provides an opportunity for the new SSI Coordinator to select an up-coming training course or request notification of future course-offerings. New SSI Coordinators who have not received notification of registration within two weeks of completing the SSI Coordinator InfoPath Form should notify SSI@tsa.dhs.gov.

Note: Assessments of SSI documents may not be completed until after SSI Coordinators become SSI Certified. If an office requests that a new SSI Coordinator complete an SSI Assessment before becoming SSI Certified, the SSI Coordinator should submit the review through the SSI Program Review Request Form.

SSI Coordinator's Roles and Responsibilities

After completing and successfully passing the Advanced SSI Training and Certification Course, the SSI Coordinator will receive an invite to attend the "SSI Coordinator's Roles and Responsibilities" course. This course provides valuable information and instructions on SSI Coordinator roles and responsibilities. A play-back of this Webinar will be available in the SSI Coordinator's Library.

Appendix 10: Instructions for Certified SSI Coordinators

Certified SSI Coordinators should submit any requested contact information changes to the SSI Program through the SSI Coordinator InfoPath Form along with any changes to status as an SSI Coordinator or changes to scope of responsibilities (e.g., change of airports).

Maintaining Certification – Continuing Education of SSI (CESSI)

SSI Certified Coordinators are required to participate in CESSI activities throughout the year. All Certified SSI Coordinators must earn 50 CESSI credits to maintain certification. A list of CESSI activities can be found on the SSI iShare page.

- Types of activities that Certified Coordinators can do to earn credit are distributing and *posting BOLOs, attending the SSI Bi-Monthly Teleconferences, participate and promote SSI Awareness Week, attend CESSI training sessions, conducting Self Compliance Checklist audits, training stakeholders*, just to name a few. Each of these types of activities count for 3 to 15 CESSI credits. Click here to see the list of CESSI Activities.
- Each SSI Certified Coordinator must enter and track their CESSI activities utilizing the CESSI Tracker. Instructions are posted on our iShare page.
- The SSI Program will send courtesy reminders to SSI Coordinators whose CESSI credits are low or if they appear to be in jeopardy of losing certification.
- The SSI Program will make only three attempts to contact the SSI Coordinator by email to update their CESSI tracker with the activities they have performed throughout the year to maintain certification. If contact or updates to the SSI Coordinator CESSI credits have not been made, the SSI Coordinator may lose certification due to lack of maintaining certification.

Appendix 11: Instructions for Watermarking Files

Watermarking may be used as a tool with regard to SSI documents' identification, protection and tracking. In accordance with requirements under TSA MD 2810.1, *SSI Program* and TSA MD 2810.2, *Disclosure of SSI in the Pre-Award Acquisition Process*, the Office of Information Technology's Information Assurance and Cyber Security Division/Compliance and Policy Branch has developed the following instruction for watermarking files as needed to protect Sensitive Security Information.

- In MS Word, the official submitter/owner of the SSI document shall open the SSI file using the initial password and ensure that appropriate SSI headers and footers are incorporated into the SSI document, if not done so already.
- As part of the document lockdown process, the submitter shall incorporate and track their *restrictions to editing* password, and add a Watermarking Code and/or FIC containing the following key information:
    - In MS Word, open SSI document and click on: *Page Layout*, click *Watermark*, click *Custom Watermark,* click *Text watermark* box and place cursor inside the *Text* box and type-in the following (example): **BT**IBM**JD**014**07282014**
    - Select Color preference: Medium gray (preferable)
    - Semitransparent Box: Leave *unchecked*
    - Size: 60
    - Column 1-2: Submitter initials (**B**rian **T**homas) – this is the person sending the password-protected SSI document to the vendor.
    - Column 3-5: Receiving company name (**IBM**) - this space is for each and every unique vendor receiving the SSI document from the submitter.
    - Column 6-7: Receiving POC name (**J**ohn **D**oe) – this is the contractor/person receiving the SSI document from the submitter.
    - Column 8-10: Internal document sequence number (**014**) – the sender keeps track of all sequence numbers and submissions.
    - Column 11-12: Submission month (**07**) – month of document submission.
    - Column 13-14: Submission day (**28**) – day of document submission.
    - Column 15-18: Submission year (**2014**) - year of document submission.
    - NOTE: This Watermark Code/FIC shall be placed at angle.
    - *Save* document
    - Lockdown of SSI document:
        - In MS Word, go to the very top of the document tool bar and click on the right-most arrow (i.e. Customize Quick Access Toolbar).
        - Unclick or disable: Save, Quick Print, Print Review and Print and Email.
        - Save document
    - Restrict Editing Password:
        - Go to *Review* tab
        - Click on *Restrict Editing* (upper far right-hand side)
        - Item 2. Click box to "*Allow only this type of editing in the document*".
        - Select "*No Changes (Read Only)*"
        - Item 3. Start Enforcement: Click on "Yes, Start Enforcing Protection".
            - Select AND TRACK the selected password. (see subsection 5.3.2 *Creating Passwords to Encrypt SSI.*
        - Save MS Word SSI document. Closely track all passwords and place document in a secure place

Appendix 12: Formal Appeal Justification

When filing a formal appeal of SSI Determination to the SSI Program, refer to section 3.8 *SSI Challenge and Appeals Process*. The below template, also found on iShare, may be used when submitting a formal appeal of SSI determinations.

TSA SSI Program Review of XXX Markings Add Title of Review and Review Number				
Ref[1]	Page[2]	Text in Question[3]	TSA Comments	Name (SSI Challenger) Comment

[1] Citation from 49 CFR Part 1520
[2] Page from Review to be reconsidered
[3] Text at issue – Text to be reconsidered